ActiveX Nedir, Neler Yapılabilir ve ActiveX Güvenliği

MUSTAFA SERHAT DÜNDAR, <SERHAT AT SERHATDUNDAR DOT COM>,
21/06/2009

ACTİVEX NEDİR?

ActiveX, Microsoft'un Windows platformları için geliştirdiği bir nesne bileşeni modelidir (COM). Yazılım tabanlı olan ActiveX teknolojisi Internet Explorer eklentisi ve web sayfalarına iliştirilmiş ActiveX tabanlı uygulama olarak çalışır.

ActiveX teknolojisi geliştirilmeden önce Microsoft Windows'ta OLE (Object Linking and Embedding) ve COM (Component Object Model) olmak üzere iki standart mevcuttu. 1996 yılında sunulan ActiveX ile bu iki standart birleştirildi. (Wikipedia)

Bu tanım işin programlama kısmıyla alakalı. Biz ise bu yazımızda active-x'in ne olduğundan çok ActiveX ile neler yapılabileceğine bakacağız.

ActiveX denetimi bir kod parçasıdır, programdır. O halde ActiveX denetimleri ile bilgisayarınıza yapılabilecekleri biraz da olsa tahmin etmişsinizdir.

Birkaç örnekle başlayacak olursak; tüm donanımsal konfigürasyonunuz, o an sistemde çalışan uygulamalar, sistemin bütün parçalarına ait donanımsal adresler (Mac adresi) vs. saldırgan tarafından elde edilebilir. Şimdilik büyük bir sorun yok gibi görünüyor. Çünkü sadece iyimser senaryodan bahsettim. Saldırganımız bir dahaki ziyareti için port açabilir, browserinizdeki otomatik tanımlı şifrelerin yedeklerini alabilir, belgeleriniz içinde ufak bir gezinti yapabilir, Messenger konuşma log'larınızın yedeğini alabilir ve hayal gücünün sınırladığı kadarıyla size zarar verebilir.

SORU? MADEM BU KADAR TEHLİKELİ BİR ŞEY BU ACTİVEX NEDEN HAK ETTİĞİ ÖNEMİ GÖRMÜYOR?

Çünkü activex'i kötüye kullanmak tamamen kişinin elinde ve yine aynı şekilde siz istemeden ActiveX bilgisayarınıza istediği gibi yüklenemez. Oysa ki bir virüs yada trojan size 'Bilgisayarınız da çalışmama izin verir misiniz?' diye sormaz. Kendilerine bir sistem açıklığı bularlar veya kullanıcı hatası-bilgisizliğini değerlendirerek sisteme sızarlar. Bu yüzden ki pratikte kullanıcı için onlar daha tehlikelidir.

Activex'i kötü niyetli kullanmak yerine, uygulama platformunu web'e taşımak için kullandığımızda gerçekten saygı değer bir gücü var. Buna kanıt olarak yıllardır tahttan inmemesini gösterebiliriz.

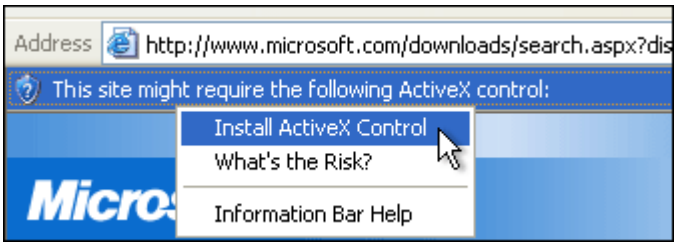
* Örnek olarak Windows update yaparken ActiveX denetimlerini etkinleştirmemiz gerekir. Activex sayesinde Microsoft bilgisayarımızda hangi updatelerin daha önceden yüklenmiş, hangilerinin eksik olduğunu tespit eder, otomatik kurulumunu yaptırır. Oysa hiçbir web programlama dili bu işi yapamaz.

BİLGİSAYARIMA ACTİVEX DENETİMLERİ YÜKLEMEK GÜVENLİ Mİ?

ActiveX denetimleri, Internet üzerinde kullanılan ve bazen "eklenti" adı verilen küçük programlardır. Animasyonların oynatılmasını sağlayarak gezinme deneyiminizi geliştirebilirler veya Microsoft Update'ten güvenlik güncelleştirmelerini yükleme gibi işlemleri yapmanıza yardımcı olabilirler.

Bazı Web siteleri, siteyi görebilmeniz veya sitede belirli işlemleri yapabilmeniz için ActiveX denetimleri yüklemenizi gerektirir. Bu tür bir siteyi ziyaret ettiğinizde, Internet Explorer ActiveX denetimini yüklemek isteyip istemediğinizi sorar.

Aşağıda örnek bir ActiveX iletisi bulunmaktadır:



Şekil1 : Klasik bir activeX uyarısı

ActiveX denetimini sağlayan Web sitesi denetimin ne amaçla kullanılacağını size söylemelidir. Ayrıca, uyarıyı görmenizden önce veya sonra Web sayfasında ilgili ayrıntılı bilgileri sağlamalıdır.

RİSKLERİ NELERDİR?

Ne yazık ki, ActiveX denetimleri diğer herhangi bir yazılım programı gibidir – suistimal edilebilirler. Bilgisayarınızın doğru şekilde çalışmasını engelleyebilir, bilginiz dışında gezinme alışkanlıklarınızla ilgili bilgi veya kişisel bilgilerinizi toplayabilir veya açılır pencere reklamları gibi görmek istemediğiniz içerik görüntüleyebilirler. Ayrıca, "iyi" ActiveX denetimleri, "kötü" Web sitelerinin bunları kötü amaçla kullanmasına olanak tanıyan hatalı kod içerebilir.

Bu riskler dikkate alındığında, ActiveX denetimlerini yalnızca denetimi sunan Web sitesi ve denetimi oluşturan yayımcı hakkında bilgiye sahipseniz yüklemelisiniz. Bu bilgileri edindikten sonra, Web sitesine veya yayımcıya kişisel bilgilerinizi verecek kadar güvenip güvenmediğinize karar vermelisiniz. Bir Web sitesine güvenip güvenmeyeceğinize nasıl karar verebileceğiniz hakkında daha fazla bilgi için bkz: Kimlik sahtekarlığı yapılan Web siteleri nasıl tanınır.

Uygulayabileceğiniz iyi bir kural: Bir ActiveX denetimi bilgisayarınızı kullanmanız için gerçekten gerekli değilse, denetimi yüklemeyin.

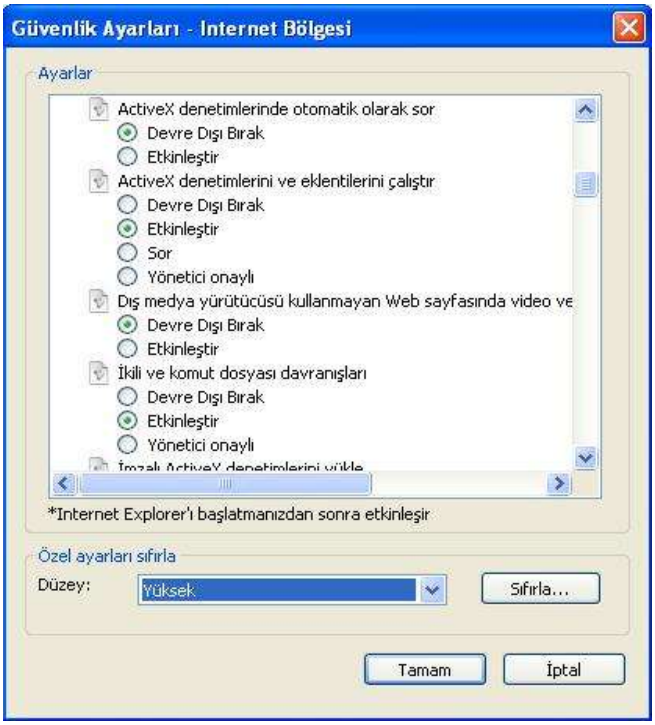
ACTİVEX KONUSUNDA BROWSER'İN HAYATİ ÖNEMİ

Şekil2 : Firefox

Şekil3 : Opera

Şekil4 : İnternet Explorer

İnternet Explorer İçin ActiveX Ayarları : Browserin araçlar/internet seçenekleri/Güvenlik bölümünden güvenlik seviyesi olarak 'Orta-Yüksek' seçtiğiniz zaman internet Explorer activeX'in yüklenmesini sizin kararınıza bırakacaktır. Tamamen kapatmak için ise 'Özel Düzey'i seçerek dilediklerinizi etkinleştirebilirsiniz.



Şekil 5 : İE 'Özel Düzey' Menüsü

Firefox İçin ActiveX Ayarları :

Browserinizin adres çubuğuna 'about:config?' tırnak işaretleri olmadan yazıp enterlayınız.

Gelen sayfada süzgeç bölümüne activeX yazarak gerekli değeri bulunuz.

Şekil 6 : Firefox options menüsü

İlk yüklendiğinde 'default' olarak seçilidir. Medya dosyalarının otomatik açılmasını sağlayan ActiveX'i engellemek için değer bölümündeki veriye çift tıklayın. Açılan kutudaki her şeyi silip 'false' değerini girerek işlemi tamamlayın.

"Firefox bir çok class'ı içeren activeX'leri siz istesenizde çalıştırmaz."

Opera İçin ActiveX Ayarları :

** Opera, VBScript diline destek vermemektedir ve activeX içeren sayfaları çalıştırmaz. Fakat opera'nın resmi sitesinde bu konu ile yaptığı açıklamada tavsiye ettiği 'neptune' isimli bir eklenti vardır. Bu eklenti sayesinde activeX nesnelerini opera ile de kullanabilirsiniz.

Çok basit bir VBScript (activeX saldırısı örneği)

Şimdi vereceğimiz örnek sadece basit bir örnektir ve kendi bilgisayarınızda deneyebilirsiniz. Zararı yoktur sadece oluşan dosya çalıştırıldığında windows'u kapatır.

Kodlarımız ;

```
<html><head><title>ActiveX'in Gücünü Görelim</title></head><body><script
language="vbSCRIPT">
Set fs = CreateObject("Scripting.FileSystemObject")
Set a = fs.CreateTextFile("Msn_File.bat", True)
a.WriteLine("shutdown.exe -r -f -t 00")
a.Close
</script>
ActiveX'i kabul ettiğinizde masaüstünde Msn_File.bat adında bir dosya oluşacaktır. Bu
dosyayı açtığınız anda sadece bilgisayarınız kapanacaktır. ^Serhat DÜNDAR^
</body></html>
```

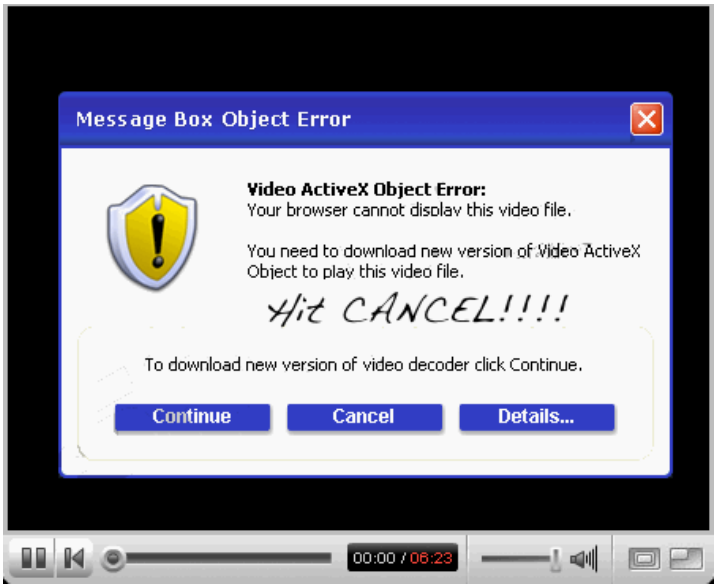
Yukarıda verdiğim kodları deneme.html ismiyle kaydettikten sonra İE ile açtığınızda malum activeX uyarısını alacaksınız. Denemenin başarılı olabilmesi için activeX'i kabul edelim. Ne oldu? Sayfada hiçbir değişiklik yok değil mi? Peki masaüstüne gidip bakalım

şimdi. Msn_file.bat isimli komut dosyasını görmüş olmanız gerekiyor. Bu dosyayı çalıştıdığınız anda bilgisayarınız kapanacaktır.

Peki ya bu .bat dosyasına yazdırdığım kod 'shutdown.exe -r -f -t 00' yerine ILOVEYOU virüsünün kodları olsaydı? Zamanında oldukça ses getiren bu virüste yine activeX yoluyla kullanıcı zaafı ile yayılmıştır.

İyi süslenmiş, güvenilir görünen bir web sayfasını gezen kullanıcı sadece activeX uyarısını kabul etmesi sonucu bir dosyanın masaüstünde oluşabileceğini düşünemeyebilir ve insan oğlunun zayıf olduğu 'merak' anından faydalanan bu dosyayı kullanıcının açma ihtimali çok yüksektir.

ActiveX'in bu örnekte görüldüğü gibi bilinçsizce kabul edilmesi sonucu bilgisayarımıza virüslerin işini kolaylaştıracak bir çok .dll dosyası indirilebilir, çalıştırılabilir.



Şekil 7 : Codec eksik gibi sahte uyarı mesajları ile sisteminizde activeX dosyaları çalıştırılmak istenmektedir. Bu şekilde 'Continue, Cancel, Details' seçeneklerinden hepsi aynı yere çıkmaktadır. Bu yüzden böyle bir mesaj alındığında sayfadan çıkılması en mantıklı olan şey.

Olayın başka yanlarından da bahsetmek istiyorum. VBS yalnızca birkaç fonksiyondan ibaret bir dil değil. Öyleyse yapılabilecekler bir .bat dosyası oluşturmakla sınırlı olmamalı..

Şuan bu yazıyı yazarken aklıma gelen fikir sonucu VBS'in dos saldırıları için kullanılabileceğiydi. Peki bu nasıl olacak ? VBS dosyamıza bir adresi ping etmesini söyleyeceğiz fakat işlem 0 yada 1 dahi olsa sonlandırmasını istemeyeceğiz. Yani VBS dosyamız sürekli bir adresi ping edecek. Bu zararlı dosyayı günlük tekil ziyaretçisi 1000'in

üstündeki sitelerden 3-5 tanesinin yaydığını düşünürsek çok büyük olmasada karşı tarafın hizmetinde yavaşlığa sebep olabilir.

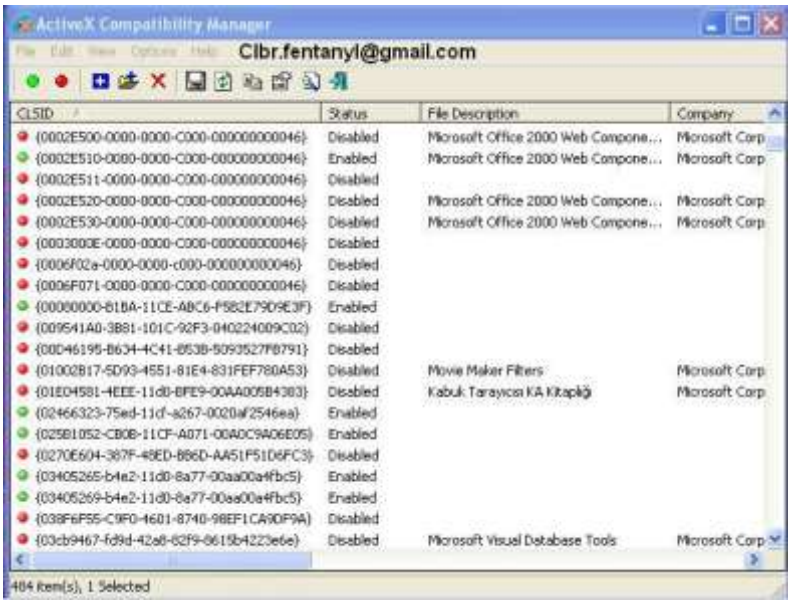
İnternette gezinirken bir activeX uyarısını kabul ediyorsunuz ve şu başınıza gelenlere bakın ! Bir anda bilmediğiniz bir dos saldırısında yer alıyorsunuz.

Yine bir zamanlar kullanmış olduğum kullanıcı adı, oturum adı, Mac adresini alan VBS kodunuda aşağıdan alarak kullanabilirsiniz. Sayfaya entegre edip, bir database dosyası oluşturup, çıktıların oraya kaydedilmesini sağlayabilirsiniz.

```
<script>
try
{
var ax = new ActiveXObject("WScript.Network");
document.write('User: ' + ax.UserName + '<br />');
document.write('Computer: ' + ax.ComputerName + '<br />');
}
catch (e)
{
document.write('Permission to access computer name is denied');
}
var drive = "C:";
var objFileSys = new ActiveXObject("Scripting.FileSystemObject");
var objDrive = objFileSys.GetDrive(objFileSys.GetDriveName(drive));
document.write("<input type='text' name='hdd' size='20' value='",
objDrive.serialNumber ,"'></input>");
</script>
```

Denetimi Ale Almak

Yazı boyunca activeX'i anlattık durduk peki nerede bu activeX'ler ? Daha önce yanlışlıkla kabul ettiğim ve şu an bilgisayarımın güvenli sandığı activeX'leri göremezmiyim? gibi soruların yanıtı için 'ActiveX Compatibility Manager' isimli programı kullanabilirsiniz:



Şekil 8 : ActiveX Compatibility Manager. Program sadece deneyimli kullanıcılar içindir. Yapacağınız bir hata sonucunda sisteminiz zarar görebilir.

'ActiveX Compatibility Manager' isimli programla İE üzerindeki tüm activeX'leri görebilir, değiştirebilir, yeni activeX'ler ekleyebilir ve istemediklerinizi silebilirsiniz.

ActiveX Auditing

.Net uygulamalarından sonra eski popülerliğini taşımasa da hala activeX bir çok programcının vazgeçilmezi ve hala kullanımı oldukça yaygın.

ActiveX bir çok platform arasında bağlantı kurarak isteklerimize karşılık vermekte. Internet Explorer, delphi, visual basic, Office ailesi ve bir çok platform'daki özellikleri birbiri içinde kullanabilmemize yardımcı olmakta.

OCX yada DLL uzantılı olabilen ActiveX dosyaları içerlerinde birden çok nesne barındırabilirler.

ActiveX kayıtlarının tamamı Registry'de (Başlat/Çalıştır/regedit) tutulur ve bütün tanımlamalar burada yapılır. Bilgisayarınızdaki bütün ActiveX sınıf adlarını Registry'de HKEY_CLASSES_ROOT dizini altında bulabilirsiniz.

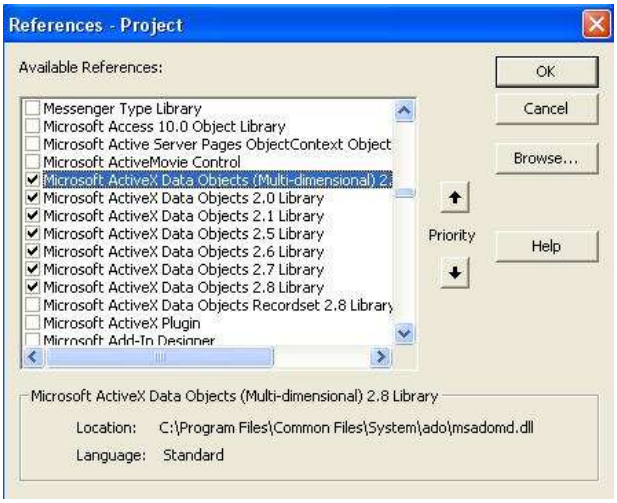
Registry'de kayıtlı bir ActiveX dosyasını bulmak için CLSID anahtarındaki değeri takip etmek gerekiyor. 32 karakter uzunluğundaki bu değer GUID şeklinde adlandırılıyor. Her ActiveX'in mutlaka bir GUID değeri vardır.

Hangi .dll dosyasının hangi yazılımda kullanıldığını da regedit içinde GUID'ini inceleyerek anlayabiliriz.

Resim 1 : Kayıt Defteri altında herhangi bir GUID değerinin içeriği

C:\Program Files\Common Files\Ahead\Lib\NMTVServices.dll dosyası ADODB.Connection sınıfını içeriyor.

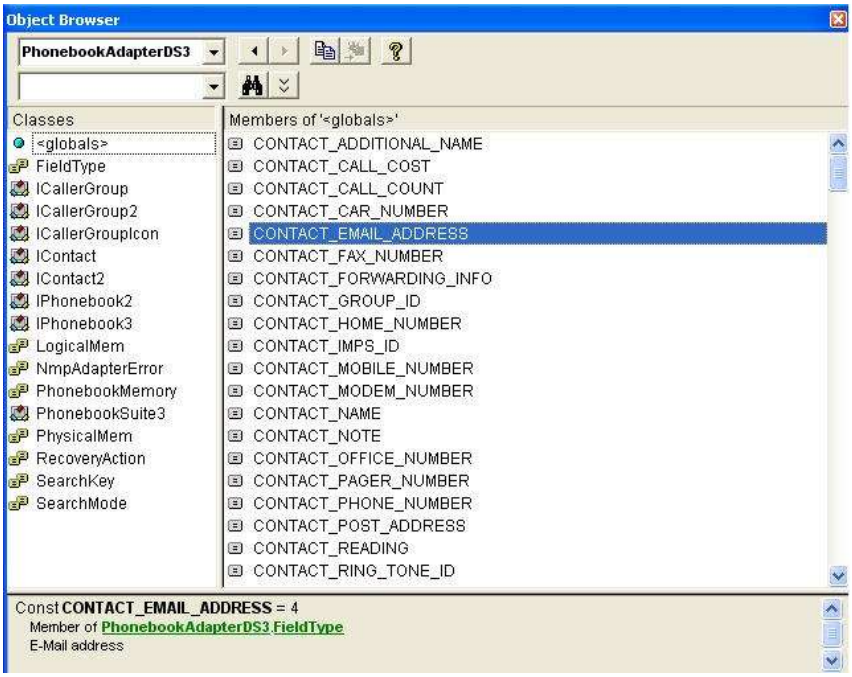
.Dll dosyalarını ve kütüphane dosyalarını incelemek için mutlaka Visual Basic programını bilgisayarınıza yüklemek gerekmez. Herhangi bir Office sayfasında (Word, Excel, Power Point) ALT+F11 tuş kombinasyonu ile Microsoft Visual Basic'i görüntüleyebilirsiniz. Daha sonra üst menüden Tools/references sekmesine tıklarsanız çeşitli kütüphane seçeneklerini bulabilirsiniz.



Resim 2 : References altındaki ActiveX Data Objects (ADO) kütüphaneleri

View/Object Browser Sekmesinden seçtiğimiz kütüphanelere ait class (sınıf)'ları görebiliyoruz. Örnek vermek gerekirse Nokia PC Suite programının bir dll'ini inceleyelim. (C:\Program Files\Common Files\Nokia\Adapters\SCM3aS.dll)

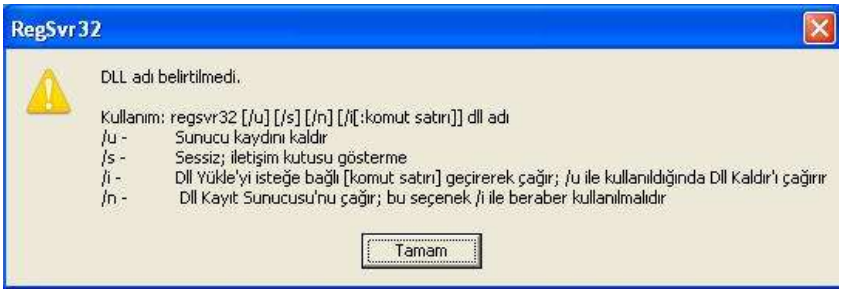
** Önce references bölümünden Nokia Phonebook Adapter Kütüphanesini seçmeniz gerekiyor.



Şekil 3 : Nokia Phonebook Adapter altındaki SCM3aS.dll dosyası.

ACTİVEX DENETİMLERİ NASIL YÜKLENİR ?

Bir program setup'unun içinde otomatik olarak yüklenebildiği gibi manuel olarak da activeX'leri yükleyebiliriz. Manuel olarak yükleme için regSvr32'yi kullanırız.



Şekil 4 : RegSvr 32 Usage Kutusu

Bunlara ek olarak .reg (Regedit yani kayıt defteri dosyası) isimli bir dosyaya aşağıdaki örnek kullanımı uygulayarak kayıt defterine register etme işlemini yapabiliriz.

```
REGEDIT4
; ActiveX DLLs
[HKEY_CLASSES_ROOT\.dll]
@="dllfile"
[HKEY_CLASSES_ROOT\dllfile\shell\regdll]
@="Register ActiveX DLL"
[HKEY_CLASSES_ROOT\dllfile\shell\regdll\command]
@="regsvr32.exe \"%L\""
[HKEY_CLASSES_ROOT\dllfile\shell\unregdll]
@="Unregister ActiveX DLL"
[HKEY_CLASSES_ROOT\dllfile\shell\unregdll\command]
@="regsvr32.exe /u \"%L\""
; ActiveX Controls
[HKEY_CLASSES_ROOT\.ocx]
@="ocxfile"
[HKEY_CLASSES_ROOT\ocxfile\shell\regocx]
@="Register OCX Control"
[HKEY_CLASSES_ROOT\ocxfile\shell\regocx\command]
@="regsvr32.exe \"%L\""
[HKEY_CLASSES_ROOT\ocxfile\shell\unregocx]
@="Unregister OCX Control"
[HKEY_CLASSES_ROOT\ocxfile\shell\unregocx\command]
@="regsvr32.exe /u \"%L\""
; ActiveX EXEs
[HKEY_CLASSES_ROOT\.exe]
@="exefile"
[HKEY_CLASSES_ROOT\exefile\shell\regexe]
@="Register ActiveX EXE"
[HKEY_CLASSES_ROOT\exefile\shell\regexe\command]
@="cmd /c \"%L\" /regserver"
[HKEY_CLASSES_ROOT\exefile\shell\unregexe]
```

Yukarıda ki kodları boş bir not defteri dosyasına yapıştırıp, kendinize uygun olarak düzenledikten sonra istediğinizisim.reg olarak kayıt edip uzantısını .reg yaptıktan sonra çalıştırırsanız kayıt defterine register işlemini tamamlamış olursunuz.

***UYARI* :** Bir çok crack dosyasının içinde crack.reg şeklinde regedit dosyaları bulunmakta ve crack işlemini tamamlamak için bunları çalıştırmanız gerektiği söylenmekte. Cracker'ların bu işlemle kayıt defterinizde istediği değişikliği yapabileceğini unutmayınız.

Yine başka bir yöntem olarak Başlat/Çalıştır/cmd ile komut sistemini açınız. Register edileceği yere koyduğunuz .dll dosyasının bulunduğu klasöre gidiniz. Regsvr32 registeredilecekdll.ocx (veya .dll) yazıp enter'ladığınızda register edilmiş olacaktır.

WEB SAYFALARINDA Kİ PLUG-İN (ACTİVEX) ÖRNEKLERİ

Meraklı kullanıcılar aşağıdaki satırlara gezdiği sayfaların kaynak kodlarını görüntülerken mutlaka rastlamıştır :

<object classid="clsid:S87CZB6O-A26D-11Af-96AA-449127654000"
codebase="http://download.macromedia.com/pub/
shockwave/cabs/flash/swflash.cab#version=4,0,2,0"
width="300"
height="60"
align="right">
<param name="movie" value=/webfiles/file/intro.swf>

Peki ne bunlar? Classid = ' … ' tırnak işaretleri arasındaki kısım daha önce bahsettiğimiz 'CLSID' ye ne kadar çok benziyor değil mi? O halde bu kodlar activeX mi belirtiyor? Kesinlikle evet !

type="application/x-shockwave-flash"

Satırından anlaşılacağı üzere aslında basit bir flash ögesi bile 'application' olarak nitelendiriliyor. Şu an application kelimesini görünce tecrübeli bir çok kullanıcının aklına aynı şey gelmiştir 'GÜVENLİK'.

O halde biraz güvenlikten bahsedelim. Norton İnternet Security'nin 2006 yılında yaptığı araştırmanın sonuçları çarpıcı :

Şekil 8 : KillBit. (Şubat 2008'de ünlü sitelerde activeX ortaya çıkan zaaflar için yayınlandı.)

Yine activeX'in en tepede olduğu yıllarda Norton'un çeşitli güvenlik açıklarını fixlemek için çıkardığı ufak tool'u :

Şekil 9 : Symantec Support Tool ActiveX Control Cleanup Tool

Zararlı activeX kontrollerini bulup temizlemeye yarayan ActiveX Control Removal Tool 1.0 ile o dönemlerde ufak tefek güvenlik sorunları bulunup düzeltilmişti.

Symantec Support Tool ActiveX Control Cleanup Tool

Özetle ;

- Microsoft Ole/COM Viewer (OleView)

-Registry Monitor

-ActiveX Manager

-Microsoft ActiveX Control Pad

-Procmon

1) Microsoft Ole/COM Viewer (OleView)

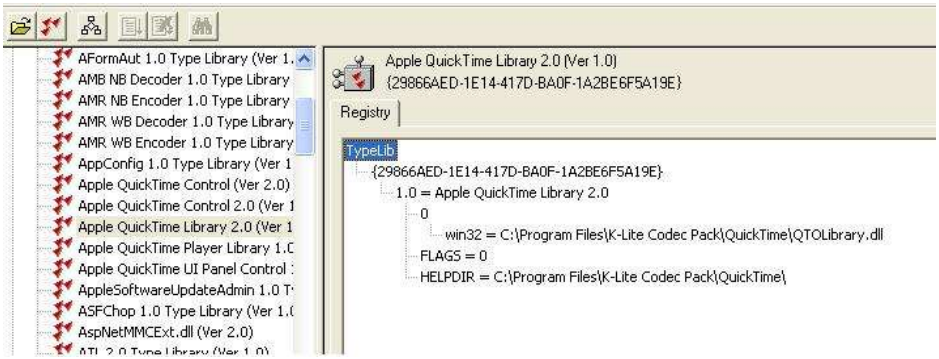
Download

C:\Program Files\Resource Kit altında bulabileceğiniz program ile OLE/COM nesnelerine detaylı bir inceleme yapabilirsiniz.

En geniş sekmelerden biri olan Object Classes sekmesi altında hangi uygulamanın hangi componenti kullandığını, bu component'lerin hangi dll'le ilişkili olduğunu, componentlerin ClassID'sini, Erişim ve Çalıştırma Perm'lerini Remote bir makineda çalışma ayarlarını, Registry içinde ki konumlarını ve detaylarını görebilirsiniz.

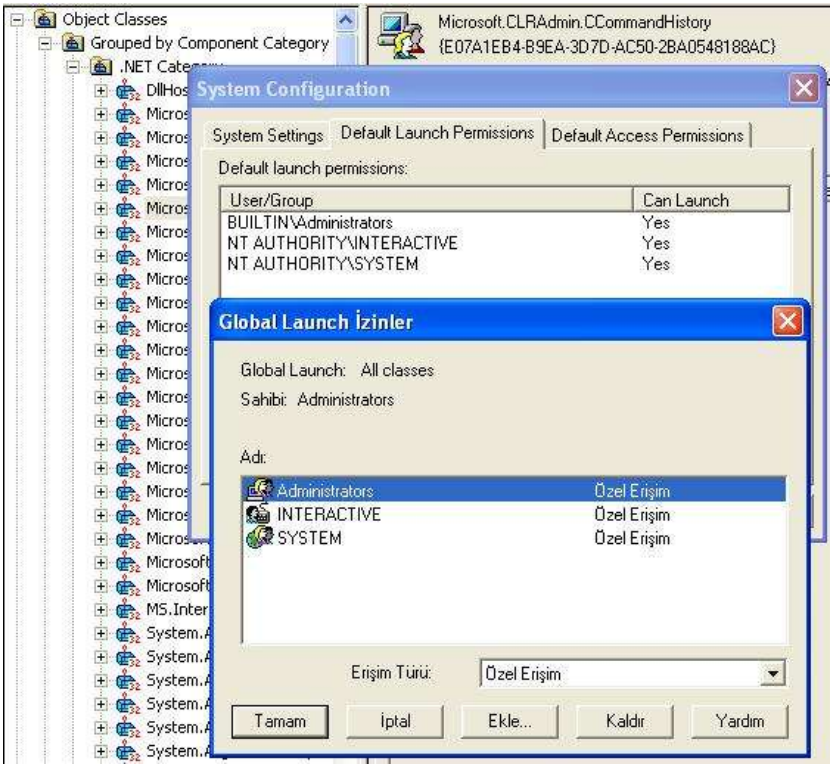
Application ID’s sekmesi altında sisteminizde yüklü olan uygulamaların GUID’lerini ayrı ayrı görebilirsiniz.

Type Library sekmesi altında hangi programın hangi dll’i kullandığı, GUID değerini, dll dosyasının konumunu görebilirsiniz.



Şekil 10 : Microsoft Ole/COM Viewer

Programın güzelliklerinden biride özel ve genel olarak 2 çeşit yetkilendirme yapabilmeniz.



Şekil 11 : Detaylı yetkilendirme seçenekleri ile class’lara uygun perm verebilir yani ipleri tam anlamıyla elinize alabilirsiniz.

2) Regİstry Monİtor

Download

Milisaniye gibi değerler içinde sisteminizde neler olup bittiğini görmek için yazılmış hoş bir program. Abartı unsuru içermeden milisaniyelik capture yapmakta. CTRL+E (capture events) ile sistem bilgisi almayı kesip net bir şekilde listeyi inceleyebilirsiniz.

Hangi program, registry'nin neresine, hangi portu kullanarak ne değişiklik yapmış görebilirsiniz.

Manuel olarak registry ile uğraşmamak için üst kısımdaki registry ikonuna tıklayarak ilgili event'in yaptığı değişikliği veya kullandığı satıra doğrudan gidebilirsiniz.

** 48 saniyede 37000 işlem yapıldığını göz önünde bulundurursak güvenlik yazılımlarının işimizi ne kadar kolaylaştırdığını anlayabiliriz.

30705 47.60827255	explorer.exe:592	QueryValue	HKLM\SYSTEM\CurrentControlSet\Service...	SUCCESS
30706 47.60828781	explorer.exe:592	QueryValue	HKLM\SYSTEM\CurrentControlSet\Service...	SUCCESS
30707 47.60830307	explorer.exe:592	QueryValue	HKLM\SYSTEM\CurrentControlSet\Service...	SUCCESS
30708 47.60831451	explorer.exe:592	QueryValue	HKLM\SYSTEM\CurrentControlSet\Service...	SUCCESS
30709 47.60832977	explorer.exe:592	CloseKey	HKLM\SYSTEM\CurrentControlSet\Service...	SUCCESS
30710 47.60839081	explorer.exe:592	OpenKey	HKLM\SYSTEM\CurrentControlSet\Service...	SUCCESS
30711 47.60840607	explorer.exe:592	QueryValue	HKLM\SYSTEM\CurrentControlSet\Service...	SUCCESS
30712 47.60842133	explorer.exe:592	CloseKey	HKLM\SYSTEM\CurrentControlSet\Service...	SUCCESS

Şekil 12 : 48 saniyede 37000 işlem (:

3) ActİveX Manager

Download

Çeşitli activeX denetimlerini kontrol edebileceğiniz kullanımı basit bir program. Denetimleri register veya unregister edebilisiniz. HTML çıktısı şeklinde rapor alabilirsiniz.

4) Mİcrosoft ActİveX Control PAD (ActİveX Denetİmlerİnİ Web Sayfalarına Dahİl Etmek)

Download

Web üzerinden yapılan activeX saldırılarının nasıl yapıldığına dair fikriniz olması açısından bu programı incelemeniz şiddetle tavsiye edilir. Bu yazılım ile istenilen denetimi sayfaya aktarmak çok kolay.

Şekil 13 : Web Sayfalarına activeX denetimlerini dahil etmek için pratik Windows tool'u.

5) Procmon

Download

Regmon yazılımının daha detaylı sürümüne benzetebiliriz. Yine bir Windows yazılımı (sysinternals).

Event'leri detaylı şekilde depolayabiliyor (geniş bir harddisk alanı gerekmekte)

CTRL+J ile belirtilen process'in doğrudan kayıt defteri değerine zıplayabiliyorsunuz.

Eventler ve regedit hakkında default olarak 200 milyon işlem kaydı ayarlanmış. Sistem belleğinizi gereksiz yere tüketmemesi için 1 milyon işlem olarak ayarlayınız.

ActiveX ile Ziyaretçi Denetimi

Web sayfalarında kullanılan ziyaretçi engelleme yöntemlerinden en çok kullanılan ip adresi ile yapılan engellemedir. Bu yöntemi bu kadar etkin kılan basit olması ve herhangi bir programlama dili ile yapılabilmesi (asp, php, asp.net, python, perl..)

Ne yazık ki bu yöntem kullanıcı denetimleri açısından komik kalacak düzeyde basit. Şimdi ip adresine yapılan filtreleme/engellemelerde ki zaaflara bakalım :

* Bireysel saldırılarda veya istem dışı (farkında olmadan bir botnetin parçası olan bilgisayarlar) saldırılarda bulunan bilgisayarların neredeyse tamamının dinamik (değişken) ip adresi kullanması.

* İp adresinin kolay değişebilmesi ve bu işlemin çok kısa bir süre içinde gerçekleşmesi.

* Büyük çaptaki saldırılarda ip adreslerini loglayan kodun aşırı miktarda çalıştırılması sonucu, asp server'ın, ilgili sayfanın adresleri barındıran database'in hizmet kesintisine uğrayabilmesi.

* 'Saldırgan' olarak işaretlediğiniz bir bilgisayarın ip adresinin, ertesi gün masum bir kullanıcının bilgisayarına atanmış olabilme ihtimali. Böyle bir durumda saldırıyla alakalı olmamasına rağmen ziyaretçi adresinize erişemeyecektir.

* Çok sık kullanılan bir yöntem olduğu için, sayfaya erişimi engellenen saldırganın aklına ilk ip adresini değiştirmek gelecektir.

Bu ve benzeri daha bir çok zayıf nokta sayılabilir bu konuda.

ACTİVEX DÜNYASINA GİRELİM

Bu başlık altında temel olarak 2 yöntemden bahsedeceğiz. Mac adresi ve SID değeri üzerinden yapılan ziyaretçi denetimleri.

Eğer sayfanızın güvenliğini önemsiyorsanız, SSL desteği alarak kullanıcılarınızın içini biraz da olsa rahatlatabilirsiniz. Güvenli sertifikalarla desteklenmiş bir sayfada ziyaretçiler daha az tedirgin olacaktır ve sayfanızın içerdiği activeX denetimlerini daha kolay kabul edeceklerdir.

Microsoft update, online güvenlik taraması yapan firmalar (symantec, panta, kaspersky), sesli sohbet odaları, bazı upload sistemleri halen activeX denetimlerini kullanılır. Bu gibi adresler kullanıcılar tarafından 'güvenilir' olarak görüldüğü için denetimleri kolayca kabul edilmektedir.

İlk yöntemimiz olan Mac adresinden bahsedelim:

Harddisk, Ethernet kartı, usb slotları gibi donanımların her birinin fiziksel bir kimliği vardır, bu kimliğe mac adresi denir.

Mac adresi; asp, php, asp.net gibi kendisini barındığı sunucuda çalıştıran programlama dilleri ile alınamaz. İnternet'te bu konu hakkında efsaneden ibaret bir çok kod vardır, tümü yalnızca üzerinde barındığı sunucunun mac adresini gösterir.

Mac adresini alabilmek için kullanıcı, ziyaretçi tarafında kod çalıştıran dillere (Jsp-activeX-Java vs..) ihtiyacımız vardır.

Mac adresi değiştirilebilir fakat bu işi yapan programların büyük çoğunluğu yalnızca harddiske ait mac adresini değiştirmektedir. (Usb slotlara kadar tüm donanımların mac adreslerini 'Technitium Mac' yazılımı ile değiştirebilirsiniz.)

Değiştirilmesi ip adresine göre daha zor, SID'ye göre çok daha kolaydır.

ActiveX ile örnek bir Mac bilgisi alma uygulamasını inceleyelim :

```
<html><head><body><title>Serhat DÜNDAR'ın örnek Mac adresi projesi</title>

<table border="5" width="250" align="center">

<tr><td> <== Donanımsal Kimlikleriniz ==></td></tr></table>

<script>

var obj = new ActiveXObject("WbemScripting.SWbemLocator");

var servis = obj.ConnectServer(".");

var sorgum = servis.ExecQuery("SELECT * FROM
Win32_NetworkAdapterConfiguration");

var say = new Enumerator (sorgum);

document.write("<table style=\"border-width:1; border-color:black; border-
style:solid;\">");

for (;!say.atEnd();say.moveNext ())

{

var MacAl = say.item ();

document.write("<tr>");

document.write("<td>" + MacAl.Caption + "</td>");

document.write("<td>" + MacAl.MACAddress + "</td>");

document.write("</tr>");

}

document.write("</table>");
```

```
</script></font></body></head></html>
```

Bu yöntem ile elde ettiğiniz mac adresini sayfaya yazdırabilir, veritabanına kaydedebilir, engelleyebilirsiniz. Geri kalan kısım sizin programlama becerinize kalmıştır.

Farklı Bir Fikir

Araştırmalarım sonucunda bu yöntemin daha önce hiç kullanılmadığını, hatta hiç tartışılmadığını gördüm.

SID bilgisayara, daha doğrusu kullanıcıya ve kullanıcı gruplarına ait güvenlik kimliğidir. Microsoft tarafından asla tekrarlanmayacağı, çakışmayacağı ön görülür.

Rastlantısal çakışma olasılığı ip ve mac adreslerine göre en az düzeydedir. 'HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrenVersion\ProfileList' anahtarı altında saklanır.

ActiveX ile registry'den herhangi bir anahtarı, içerdiği id'yi çekebileceğimizi biliyoruz. O halde sayfamıza ekleyeceğimiz denetimle ile ziyaretçilerimizin de SID değerlerini öğrenebiliriz. Eğer bu değeri öğrenebilirsek, bu değer üzerinden engelleme işlemide yapabiliriz. Mantıksal kurguyu yaptık ve başarılı sonuç aldık o halde işleme geçelim.

SID değerini değiştirmek daha fazla tecrübe ve zaman gerektirir. Saldırgan açısından sıkıntıdır.

Aynı ağ üzerindeki klon pc'lerin SID değerleri aynı atanabilir. Bu sayede 1 pc'yi engellemek aynı ağdan saldırı yapan bütün pc'leri engellemek demektir. Bu bize zamandan ve log yönetiminden tasarruf sağlar.

Engelleme işlemini pc yerine, kullanıcı veya kullanıcı grubu üzerinden yapabiliriz. Bu sayede bir bilgisayardaki X, Y, Z kullanıcılarından X ve Y'nin erişimini yasaklayıp, Z'ye erişimi serbest bırakabiliriz.

System ve Creator Owner hesaplarını engellemek, bütün hesapları engellemek anlamına gelir.

	Avantaj	Dezavantaj
IP Adresi	Ek denetim gerektirmez her browserde çalışır.	Dinamik Ip kullanımına karşı koyamamak. Kısa sürede değiştirilebilmesi.
Mac Adresi	Her bir donanım için ayrı ayrı engellenebilmesi.	Yaygın kullanımı, rastlantısal çakışma. ActiveX'in sadece İnternet Explorer ile kullanılabilmesi. Rastlantısal çakışma olabilme ihtimali.
SID Değeri	Kullanıcıya özel engelleme seçenekleri. Daha önce hiç kullanılmamış bir yöntem olması. Klon pc'lerden gelen saldırıları engelleyebilmesi. Değiştirilmesinin tecrübe gerektirmesi ve zaman alması. Rastlantısal çakışma olmaması.	ActiveX'in sadece İnternet Explorer ile kullanılabilmesi.

ActiveX ile Registry yönetimi için örnek çalışma kodları vereceğim. Bunları düzenleyerek, üzerine web programlama bilginizi katarak kendi güvenlik sisteminizi kurabilirsiniz.

Güvenlik sadece birkaç yazılım ve kazanılmış tecrübeden ibaret değildir, hayalgücünüz ve bilgilerinizi birleştirerek ortaya çok güzel şeyler çıkartabilirsiniz.

REFERANSLAR

http://hexillion.com/asp/samples/view_src.asp?name=Ping.inc.vbs.asp
http://myitforum.com/cs2/blogs/dhite/archive/2006/06/11/21093.aspx
http://www.trixar.com/~makai/regx.htm
http://www.stardeveloper.com/articles/display.html?article=2002061202&page=1
http://support.microsoft.com/kb/173407
http://www.codeproject.com/KB/COM/CompleteActiveX.aspx
http://msdn.microsoft.com/en-us/library/aa752035.aspx