Truva Atı ve Virüslerin Temizlenmesi

Ulusal Siber Olaylara Müdahale Merkezi (USOM -TRCERT)
Bilgi Teknolojileri ve İletişim Kurumu
Telekomünikasyon İletişim Başkanlığı
Tel: (0312) 586 53 05
Web: www.usom.gov.tr
E-posta: usom@usom.gov.tr

Temmuz 2014
UR.RHB.003

İÇİNDEKİLER

1. GİRİŞ

İnternette dolaşan kötücül yazılımların sayısının gün geçtikçe artmasıyla, bu tür bir yazılımın bilgisayarınıza bulaşması herkesin başına gelebilecek gündelik bir olay haline gelmiştir. Eğer hangi kötücül yazılımın bilgisayarınıza bulaştığını biliyorsanız, piyasadaki anti virüs internet sitelerini ziyaret ederek söz konusu yazılımı bilgisayarınızdan temizlemek için gerekli araçları temin edebilirsiniz. Ancak bilgisayarınıza bulaşan zararlı yazılımların tanımlanması her zaman mümkün olmayabilmektedir. Bu gibi durumlarda yapılabilecek işlemler sınırlı olmakla birlikte aşağıda belirtilen adımlar bilgisayarlarınız ve dosyalarınızı korumanızda yardımcı olabilecektir.

2. TAVSİYE EDİLEN İŞLEMLER

2.1. DESTEK BİRİMİ İLE İRTİBAT KURUN

Bulunduğunuz ortamda bilgi teknolojileri destek biriminiz mevcut ise vakit kaybetmeden irtibat kurarak, talimatlarını takip ediniz.

2.2. BİLGİSAYARINIZIN İNTERNET BAĞLANTISINI KESİN

Ne tür bir truva atı veya virüsün bilgisayarınıza bulaştığı ile bağlantılı olmak üzere, davetsiz misafirin kişisel bilgilerinize erişmesi ve bilgisayarınızı kullanarak diğer kişilerin bilgisayarına saldırması muhtemeldir. Bu tür faaliyetleri bilgisayarınızın internet bağlantısını kapatarak durdurabilirsiniz.

2.3. ÖNEMLİ DOSYALARINIZI KURTARIN

Bu noktada, dosyalarınızı yedeklemek için zaman ayırmanız önemlidir. Mümkünse eğer, tüm fotoğraflarınız, dosyalarınız ve belgeleriniz gibi bilgilerinizi bir CD'ye, DVD'ye veya başka bir harici depolama aygıtına kayıt edebilirsiniz. Ancak söz konusu yedeklenmiş bilgilerinize de kötücül yazılım bulaşmış olabilir. Bu nedenle bu tür bilgilerinizin belirli aralıklarla yedeklerini almanız halinde muhtemel bir kötücül yazılım bulaşması durumunda eski yedeklerden bilgilerinizi geri getirmeniz mümkün olabilecektir.

2.4. MAKİNENİZİ TARAYIN

Bilgisayarınıza (İşletim sisteminiz dâhil) kötücül yazılım bulaşması halinde kurtarma CD'si kullanarak bilgisayarınızı taramanız, daha önce bilgisayarınıza yüklenmiş bir anti virüs programı ile tarama yapmanızdan daha güvenli bir yoldur. Birçok anti virüs ürünü bu taramayı sağlamaktadır. Diğer bir alternatif yol ise internet tabanlı bir anti virüs silme programı kullanmanızdır. Bazı anti virüs sağlayıcıları tarafından bu tip internet tabanlı hizmetler verilmektedir. (internette "online virus scan taraması" yazarak tarama yapabilirsiniz.)

İkinci en iyi uygulama ise CD-Rom gibi kötücül yazılım bulaşmamış bir kaynaktan bilgisayarınıza bir anti virüs programı yüklemenizdir. Yazılımı yüklemeniz ardından, makinanızın taranması işlemini tamamlayınız. Tarama başlatmanız kötücül programların bulunmasında yardımcı olacaktır. İdeal olarak, anti virüs programında kötücül yazılımı bilgisayarınızdan giderme seçeneğinin bulunması beklenir. Program tarafından size sunulan tavsiye ve talimatları takip ediniz.

Eğer anti virüs programı başarılı bir şekilde kötücül dosyaları tespit ve temizlemesini yaptıysa, başka bir kötücül yazılım bulaşmasını engellemek için Adım 7'de yer verilen tedbir adımlarını takip ediniz. Anti virüs programının kötücül yazılımını tespit ve temizlenmesini sağlayamadığı durumlarda, adım 5 ve 6'yı takip etmelisiniz.

2.5. İŞLETİM SİSTEMİNİZİ TEKRAR YÜKLEYİN

Eğer bir önceki adım bilgisayarınızı temizlemeye yetmediyse, en etkili seçenek, hard diskinizi formatlamak veya tamamen silmek ve işletim sisteminizi tekrar yüklemektir. Bu işlem aynı zamanda tüm dosyalarınızın ve programlarınızın kaybolmasına neden olacaktır. Bununla birlikte bu yöntem bilgisayarınızın herhangi bir arka kapı veya davetsiz misafir içermeyecek şekilde temizlendiğinden emin olmanın tek yoludur.

Birçok bilgisayar üreticisi kurtarma diskleri gibi bilgisayarınızın fabrika ayarlarına geri dönmesini sağlamayan araçlar sunmaktadır. Konu ile ilgili bilgi edinmek amacıyla bilgisayarınızın kullanım kılavuzunu okumanız tavsiye edilir. Tekrar yüklemeyi yapmadan önce, tüm programlarınızı ve ayarlarınızı bir yere not etmeniz

bilgisayarınızın orijinal haline getirmenizde yardımcı olacaktır. Daha sonra anti virüs programınızı yüklemeniz ve bilinen güvenlik yamalarını yapmanız faydalı olacaktır.

2.6. YEDEKLENMİŞ DOSYALARINIZI YENİDEN YÜKLEYİN

Bilgisayarınızdaki bilgilerinizin yedekleri mevcut ise, artık dosyalarınızın bilgisayarınıza yeniden yükleyebilirsiniz. Bilgisayarınıza dosyaları yerleştirmeden önce, anti virüs programınız ile bilinen virüslere karşı taratabilirsiniz.

2.7. BİLGİSAYARINIZI KORUYUN

Gelecekte karşılaşacağınız virüs bulaşma durumlarına karşı, aşağıda yer verilen önlemleri almanız tavsiye edilir.

- E-Postalarınızdaki şüpheli veya tanımlayamadığınız ekleri açmayın.
- Şüpheli veya tanımlayamadığınız linkleri tıklamayın.
- Güncel anti virüs programlarını kullanın.
- Güvenlik duvarı kullanın.
- İnternet tarayıcınızla ilgili güvenlik önlemlerini alın.
- Sisteminize yeni sürümleri ve güvenlik yamalarını yükleyin.

3.KAYNAKLAR

[1] Durkota, M. D. & Dormann, W. 2008. *Recovering from a Trojan Horse or Virus.* Carnegie Mellon University.

http://www.us-cert.gov/security-publications/recovering-trojan-horse-or-virus

[2] McDowell, M. & Householder, A. 2009. *Understanding Firewalls*. Alerts and Tips.

http://www.us-cert.gov/cas/tips/ST04-004.html

[3] McDowell, M. & Householder, A. 2009. *Good Security Habits.* Alerts and Tips.

http://www.us-cert.gov/cas/tips/ST04-003.html

[4] Microsoft, *Güvenlik Merkezi.*

http://www.microsoft.com/security/default.asp

[5] US-CERT. 2001. *Home Network Security.* Publications.

http://www.us-cert.gov/reading_room/home-network-security/

[6] US-CERT. 2011.*Before You Connect a New Computer to the Internet.* Carnegie Mellon University.

http://www.us-cert.gov/reading_room/before_you_plug_in.html