Forum

Gülgûn Akbaba

Bilgisayar Zararlıları?

Virüs insanlarda olduğu gibi zararlı; bilgisayarda kolayca yayılan ve zarar veren en küçük bilgisayar yazılımları. Canlı değil; ama canlının yapmış olduğu ufak yapay zekaya sahip yazılımlar.Verilenleri istenilen ölçüde; verileni işleyen küçükcüler.

Asm (assembly), makine diliyle yazılır, tabiiii istediğiniz programlama diliyle virüs yazabilirsiniz; fakat makine dilinin zorluğu yüzünden virüsün boyutu ve esnekliği en iyi asm ile gerçekleştirilir. Yani virüs bulaşmış dediğimizde, annemizin bilgisayarını tozlu bırakıyorsun demesiyle bir ilgisi yoktur; virüs küçük zarar veren programlar diyebiliriz.

Şimdi biz bir bilgisayar programcısı olalım ve bir virüs yazalım: Sizce neleri yaparız? Ne biliyorsak o ölçüsü programcısının zekası ve bilgisine dayalı büyür. Şimdi elimizde yazdığımız bir virüs var. Ne yapacağız? Elbette yayılmasını isteyeceğiz. Bu eski yıllarda çok mümkün olmayan bir şeydi; çünkü İnternet ya yoktu ya da çok az yaygındı. O zamanlar yalnızca diskette çektiğimiz oyunlardan ya da ms-dos programlarından bulaşırdı. Şu an ise hepinizin bildiği gibi İnternet üzerinden bulaşmakta.

Virüs en küçük program demiştik; sebebi kopyalanmasındaki hızı ve dikkat çekmeden İnternetteki bir kullanıcıya kendini kabul ettirmesi; yayılması kullanılacak bir dosyayı açıp kendi kodlarını kopyalayıp o programı taşıyıcı olarak kullanarak bir zincir oluşturması, yani bu biri dur diyene kadar devam eden ve böyle milyonlarca bilgisayara ulaşan bir veri trafiğine yol açar. Elbette programcının zekası ve kodlama bilgi düzeyi isteğine bağlı olarak virüs anında ya da diyelim kopyalandıktan 20 gün sonra zarar vermeye başlar. Programcının zaman koyma sebebi de o bilgisayardan o zaman zarfı içinde başka bilgisayarlara yayılmasına yardım etmesi içindir, aynı insan hayatındaki virüsler gibi bir çoğalma dönemi vardır. O ara içinde virüs vücuda tam zarar vermez, aynı sinsilik bilgisayar virüslerinde vardır ve virüs görevine başlar. Sonuçta programlandığı için soru bile sormadan görevini yapar.

Bir virüs tamamen programcının zekasına dayalı güçlüdür, programcı boş bir sayfaya kodladığı bilgilerle güçlenir. Yani her virüs ayrıdır, ayrı şekillerde yayılır ve zarar verir. Diyebiliriz sonuçta her insan farklı düşünür, elinizdeki taşlar aynı olsa da.

Virüs Yazma Sebebleri: Programcının bilgisini kanıtlama isteği, ego tatmin, kendini geliştirmek, bilgisayar güvenlik şirketleriyle anlaşması, bilgisayar donanım üretim firmalarıyla anlaşması, siyasi örgüt ya da düşünceye destek amaçlı, büyük işletim sistemleriyle anlaşması, para kazanmak amaçlı,

Evet son beş sebebe dikkat edin. Unutulmaması gereken konu çok büyük paraların döndüğü bu beş seçenekte virüsün gereksimi çok yüksektir; çünkü virüs olmasa, güvenlik programlarına gerek duyulmaz ki. Bu programların tüm dünyaya satışı vardır. Yine aynı şekilde işletim sistemleri (isim vermiyorum), sonuçta "ben en güvenlisiyim" demesi gerekiyor; aynı şekil virüsün bilgisayar donanıma verdiği zarar üreticinin kar payını tatmin edecek oranda arttırıyor.

Aslında virüs programcılarının birçoğu para kazanan programcılardır. Sakın ben de onlardan olacağım diye atlamayın. Yasal bir meslek değil; yani mafya da para kazanır, ama "mafya olmak" iyi bir şey değildir.

Bir virüs ne yapabilir?

Aslında bu sorunun yanıtı "her şeyi"; çünki bilgisayar makine diline göre 0 1 ile kodlanmıştır. Virüs bunlarla ya da bunlarda unutulmuş düşünülmemiş hata (bug) ya da boşluklardan yanarak, oynayarak her şeyi yapar. Elbette programcının bilgi düzeyine göre. Donanıma, yazılıma, tüm verilere istediği oranda ve zamanda zarar verir.

Virüs yayma sebebi zaten düşünülürse ortaya çıkıyor. Amaç birçok bilgisayara ulaşmak ve yok edilmesini zorlaştırmak. Virüs çoğalması kendi kodunu diğer bilgisayar programın koduna işler; bunu bu programı alan diğer kullanıcı çalıştırdığı zaman, o bilgisayarda yayılmaya ondan da başka bilgisayara yayılmaya ve zarar vermeye başlar. Böyle böyle milyonlara ulaşır.

Dvd, Cd ve kilitli (Lock) zip, flash, sd kartlara, kilitli diskete bulaşamaz; çünkü bunlara hiç bir veri kopyalanamaz.Veri kopyalanamadığı için kendini de doğal olarak kopyalayamaz; yani yalnızca okuma izinli olan yardımcılara bulaşamaz.

Dünyada milyonlarca virüs yazılımı mevcut. Bu da antivirüs programlarının ortaya çıkmasını sağlar.

Anti-virüs yazılımları virüsü nasıl anlar?

En basit yöntemi yazan programcıdan çalışma ve yayılma bilgilerini alır. Ama biz düzgün çalışan firmaların yaptıklarından söz edelim. Bunlar öncelikle virüsü deneyerek, nasıl yayıldığını, ilk olarak nasıl ve nereye kendini kopyaladığını araştırır ya da virüsü oluşturan kodları çözer; böylece dönüşüm yolunu bulur; bunu bulduğunda engelleyerek, silinmesini sağlar ya da işletim sisteminde kullandığı fark edilmeyen açığı bulur ve kapatmak için ek yazılım yazar. Bu yazıldığı kadar basit değildir; arkasında birçok programcının emeği vardır. Bu yüzden destek vermek için orijinal virüs programlarını kullanmalısınız. Benim saydığım o beş seçenek "herkes için değildi" unutmayın ve siz programınızı update yaptığınızda, eğer o virüs varsa bilgisayarınızdan silinir. Buradan anlatmak istediğim konu, eğer yeni bir virüs çıkarsa ve farklı yöntemlerle çalışıyorsa ve siz anti-virüs programınızı güncellemediyseniz, virüsü kesinlikle bulamaz ve zararına sizinle eşlik eder. Bu yüzden dünya yeni yüksek düzeyde yazılmış keşfedilmemiş virüsler yüzünden donanım ve yazılım olarak zarar görür. Anti-virüs programınızı güncellemek çok önemlidir. Yalnızca anti-virüs değil, işletim sisteminizi de güncellemelisiniz. Yalnızca virüsü tanımalıyız, neyle savaştığımızı önce bilmeliyiz.

Truva atı (Trojan)

Aslında iyi amaçlı yazılan, fakat kötü amaçlı kullanılan programlardır. Birçok programlama diliyle kodlanabilir. Asıl amacı aynı ortamda olmayan farklı iki bilgisayarı İnternet ortamında buluşturmak, birbiriyle iletişimini sağlamaktır. Ana makine (server) neye bağlı olan diğer makine (client) verdiği tüm komutlara uyar ve uygular. Programcı iki program yazar: biri ana makine komutları veren diğeri komutlara uyan, client programıdır. Bu komutlar programcının bilgi ve gereksinimlerine göre yazdığı düzeydedir; ama amaç ben şirketimdeyken evimdeki bilgisayarı yönetmek istediğimde kullanmam için yazılan bu programlar sonradan kötü amaçlara hizmet etmiştir.

Trojan(Köprü)=Ana Makine(Server)+Makine(Client)

Kötü amaçlı kullanım programcının anamakine programını değişik kodlamasından doğar, yabancı olan diğer bilgisayarın kontrolü tamamen elinde olması amaçlıdır.

Neler Yapılabilir?

1. Tüm şifreleriniz alınır: Msn, icq, irc, işletim sisteminizin şifresi, dial-up ya da modem İnternet bağlantı şifreniz, bilgisayarınızda kullandığınız tüm İnternet şifreleri, mail adresleriniz, kredi kartı kullanırsanız şifre ve kredi kart no, kısaca tüm şifreleriniz.
2. Bilgisayarınız tüm kontrolü elindedir: Mouse, klavye, monitör, hdd, cdrom, webcam
3. Tüm bilgileriniz elindedir.

Kısaca bilgisayarda ne yapıyorsanız ondadır. Bu amaçla yazılmış, derlenmiş casuslardır.

Truva atı denilmesin sebebi, sizin başka program ya da bilmeden client yani komutlara uyan programı bilgisayarınıza indirmeniz ve çalıştırmanızdır. Bunlar virüsler gibi gizli değildir. Genelde .exe veya .com olan programlardır.

Worm – Spyware

Bunlar da, en kolay kaptığımız bilgisayar gribidir! Genelde işletim sistemimizin açıklarından,okunan maillerden, kullanılan p2p (paylaşım programlarından), kimi programcıların programlarına eklediği casuscuklardır. Wormlar genelde zararlı "Spyware" ise tam bir casusdur. Şimdi Spyware'in doğuş, yani yapılma amacını değinelim. Diyelim ben büyük bir web sitesiyim ya da dünya pazarında bir üreticiyim ve İnternetin en büyük reklam aracı olduğunu bilen biriyim. Milyonlarca insanı değil de, benim sitemle ilgilenen ya da ürettiğim mala ilgi duyabilecek kişileri arıyorum. İşte burada spyware devriye girer. Siz İnternette ne yapıyorsanız, karşı tarafa raporlar ve virüsler gibi de yayılma girişimlidir. Yani spyware benim ilgi alanımı ortaya çıkarır, ben film izleyen ve basketbol düşkünüysem, bunu karşıya raporlar ve bana bu dallar hakkında reklam mailleri gelmeye başlar. Elbette daha da kötü amaçlısı yok değil. Trojanda olduğu gibi tüm gizli ve para değerindeki bilgileri raporlayan spywareler de var. Ayrıca İnternet bağlantınızda belirgin bir düşüş sağlar; çünkü sizin İnternetinize ortak olarak mail ve raporlama görevlerini yapar.

Zararlı Diğer Programlar

Bunlar da programcıların isteğine bağlı olarak yazdığı kişisel programlardır. Örneğin, "Keylogger", bastığınız her tuşu kaydeder, yani yazdığınız her şeyi raporlar ve karşı tarafa iletir. Format atan, hdd kitleyen, İnternet bağlantınızı kesen zararlılardır.

Korunma Yöntemleri

Öncelikle yeni kurulmuş bir işletim sisteminin tüm güncellemelerini yapın. Anti programlarını araştırıp, istediğiniz firewall, anti-virüs, anti-spyware programlarını mutlaka kurun. Tanımadığınız mailleri açmayın ve okumayın. Size chatte gönderilen hiçbir dosyayı almayın ve girdiğiniz sitelere dikkat edin; bu önlemlerle bir ölçüde korunursuz. Kesin çözümse İnternete girmemek, hatta bilgisayarın fişini çekmektir. Bu da olmayacağından, tam çözüm yoktur.

Sessiz_cin
Delphi coder

Değerli Okurlar, görüşlerinizi
400 kelimeyi geçmeyecek biçimde ve fotoğrafınızla birlikte "TÜBİTAK Bilim ve Teknik Dergisi, Forum Köşesi, Atatürk Bul. No:221 Kavaklıdere- Ankara" adresine gönderebilirsiniz. Görüşler aktarılırken 3. şahısları suçlayıcı ifadelerden kaçınılmasını rica ederiz. Forum'da ve Serbest Kürsü'de yayımlanan okuyucu görüşleri Bilim ve Teknik dergisini bağlamaz. Forum köşesine aşağıdaki telefon ve faks numaralarıyla da erişebilirsiniz:
Tel: (312) 468 53 00 / 1067 (Gülgûn Akbaba) Faks: (312) 427 66 77