

ZARARLI YAZILIMLAR

Ahmed Semih ÖZMEKİK
171044039
HW01

BİL101 BİLGİSAYAR MÜHENDİSLİĞİNE GİRİŞ

Aslında bütününün sınıflandırılmasına çalışıldığında çeşitli amaçlar doğrultusunda birbirinden kolayca ayırabileceğimiz zararlı yazılımlar, genelinde kritik bilgileri toplamak , cihazların işleyişini bozmak ya da basitçe zarar vermek gibi amaçları güderler.

İsmi İngilizce’de “malware” yani “malicious software” tanımından alan kötücül yazılımlara 1990 yılında Yisrael Radaï tarafından bu isim verilmeden önce bilgisayar virüsü denilmekteydi.Bu şekilde adlandırmanın mantığı üzerine virüsün biyolojideki terim anlamını inceleyecek olursak; kendi başına canlılık formu göstermeyen fakat canlı bir hücreyi ele geçirip sistemin kontrolünü ele aldığında canlılık formu kazanan bir varlık olduğunu görmekteyiz.Buna bağlı olarak zararlı yazılımlara işlev katan başlıca etkenin kullanıcı tarafından en az bir defa -kandırılmak suretiyle- çalıştırılması olduğunu gözlemlediğimizde bu şekilde adlandırılmalarındaki küçük sebebi farketmek kaçınılmaz.

Tarihçesine ise küçük bir bakış attığımızda 1961 yılına kadar geri gittiğini görüp , o dönemde Victor A.Vus Satsky, Robert Morris Sr. ve M.Dsorglas gibi meraklı programcıların kendi yazdıkları programların bir bilgisayardaki depolama alanı için mücadele edip karşılıklı olarak birbirlerini sildiği, Darwin adlı bir oyun geliştirdiklerini görmekteyiz.1981’de ilk kez kavram olarak kullanılmasının yanı sıra hemen birkaç sene sonralarında Apple kullanıcılarını tekerlemelerle , ters veya yanlış mesajlarla , tamamen yersiz beliren klik sesleriyle rahatsız etmeye başlayan kötücül yazılımcılar ortaya çıkmaya başlamışlardır.Potansiyelinde sahip olduğu kötücüllüğü keşfedilemediğinden midir yoksa henüz yanlış insanların eline geçmemiş olmasından mı bilinmez ama bu yıllarda kötücül yazılımlar şuan sahip olduğu negatif imajını kazanmamışlardır.Ancak çok geçmeden 1985-1987 yılları arasında adını duyurmaya ve insanları rahatsız etmeye başlayarak bu tarihlerden günümüze kadar zararlı yazılımların şuan ki namını kazandıran bir çok olay yaşanmıştır.

Kullanım amaçlarına göre yüzeysel ve basit bir sınıflandırmayı en azından yaygın olanlarının bir kaçından örnek vererek yapmak mümkündür.

Bilgisayar Solucanı (Worm)

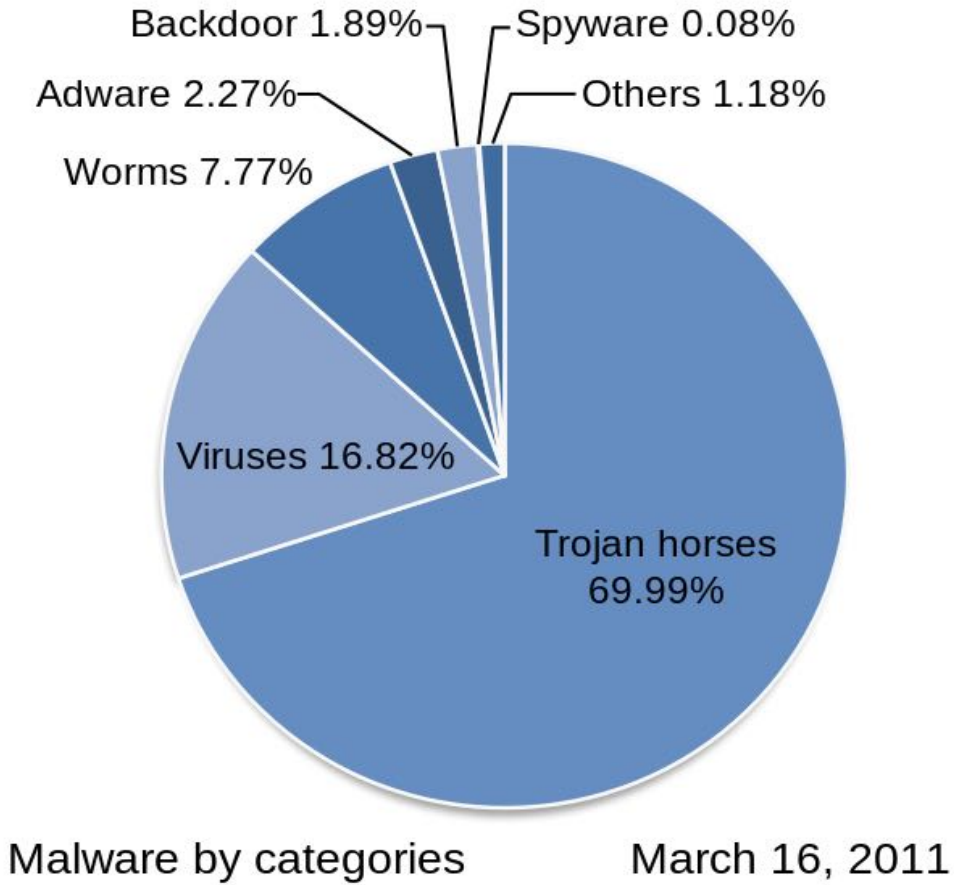
Makineye girdiğinden haberimiz olmadan, bilgisayarda dosya veya bilgi ileten özelliklerin denetimini ele geçirir ve kendi başına ilerleme özelliğiyle domino etkisiyle e-posta adresindeki kişilere kadar hızlıca yayılabilen bir tür zararlı yazılımdır.Bu domino etkisinin getirdiği yoğun ağ trafiği işyeri ağlarını ve internetin tümünü yavaşlatabilir.

Truva Atı (Trojan)

İki kısımdan oluşan,bilgisayarları uzaktan kumanda etme amacıyla yazılmış programlardır.İsmi bir efsaneden alan bu yazılımlar kendilerini kullanıcılara faydalı bir program gibi göstererek karşıdan yüklenilmesini sağlarlar ve devamında yazılma amaçlarına göre hareket ederler.

Keylogger

Keylogger basitçe klavyeden yapılan her vuruşu kaydeden ve bu kayıtları, kişisel bilgileri çalmak isteyen kişilere gönderen programdır.



Kötücül Yazılımlardan Korunmak

Kötücül yazılımların yaygınlaşmasıyla bu zararlı yazılımlara da antibiyotik etkisi yaratacak yazılımlar da korunma amaçlı olarak beraberinde gecikmemiştir. Anti-virus ve Anti-malware yazılımları olarak bilinen yazılımların amacı kötü amaçlı yazılımların, yazılım hatalarını istismar etmeden veya beklenmedik işletim sistemi davranışını tetiklemeden önce durdurmaaktır.

Gelişen bilim ve teknoloji çağında kötülüklerin de her zaman bu gelişen bu platformda kendilerine küçük yerler edineceği kaçınılmaz bir gerçektir. Dijital ortamlarda kimliğimizi ,

BİL101 BİLGİSAYAR MÜHENDİSLİĞİNE GİRİŞ

önemli bilgilerimizi , şifrelerimizi ele geçirmek isteyen kişilerin olduğunun farkındalığıyla tıpkı gündelik hayattaki dikkatimizi aynı şekilde bu ortamlara da taşımalı ve ne yaptığımızın çoğu zaman bilincinde olmalıyız.