T.C.
MALTEPE ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

BİLGİSAYAR AĞLARINDA AÇIK KAYNAK KODLU GÜVENLİK YAZILIMLARI İLE ANTI-SPAM MODÜLÜNÜN GELİŞTİRİLMESİ

YÜKSEK LİSANS(MASTER) TEZİ

Hazırlayan

Önder ŞAHİNASLAN

Tez Danışmanı

Prof.Dr. Mesut RAZBONYALI

İstanbul - 2007

T.C.
MALTEPE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

BİLGİSAYAR AĞLARINDA AÇIK KAYNAK KODLU GÜVENLİK YAZILIMLARI İLE ANTI-SPAM MODÜLÜNÜN GELİŞTİRİLMESİ

YÜKSEK LİSANS(MASTER) TEZİ

Hazırlayan

Önder ŞAHİNASLAN

Tez Danışmanı

Prof. Dr. Mesut RAZBONYALI

İstanbul - 2007

Bu tez çalışması, Maltepe Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulu'nun..... / ..... / ..... tarih ve ..... / ..... sayılı kararıyla oluşturulan jüri tarafından ***Bilgisayar Mühendisliği Yüksek Lisansı Tezi*** olarak kabul edilmiştir.

JÜRİ

Prof. Dr. A. Mesut RAZBONYALI
Danışman

Prof.Dr. Kemal KÖYMEN
Üye

Prof.Dr. İlhami YAVUZ
Üye

ÖZET

Yüksek Lisans Tezi, Bilgisayar Ağlarında Açık Kaynak Kodlu Güvenlik Yazılımları İle Anti-Spam Modülünün Geliştirilmesi, T.C. Maltepe Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı.

Bilgisayar ve internet teknolojilerinin yaygın kullanımı ile birlikte verilere erişim merkezi ve sınırlı olmaktan çıkmış ağ ortamında uzak mesafelerde dağınık paylaşılabilir hale gelmiştir. Buna e-posta ve web üzerinden gelebilecek tehditlerin eklenmesi sonucu, bilgi güvenliği ciddi bir nitelik ve boyut değişimine uğramış, önemini daha da artırmıştır.

Bireysel internet erişiminin hızlanması ve ucuzlaması ile birlikte ağa bağlı kullanıcı sayısı sürekli artmakta olup, zararlı yazılımların hareket alanı da genişlemektedir. Kötü niyetli kişilerin masum kişilerle kolay ve hızlı etkileşim kurma imkânı veren bu ortam; amaç dışı, yanlış, yanıltıcı, zararlı ve olumsuz öğeleri içeren teknolojik bir savaş haline gelmiştir. E-posta dünyanın en büyük ve en eski elektronik haberleşme yöntemi olup mesaj okuma, saklama, gonderme, sıraya koyma, randevu ve yanıtlama amaçlı kullanılmaktadır. Etkileşimli ve sürekli artış gösteren bu iletişimin farkında olan virüs yazılımcıları ve dolandırıcılar, e-posta yolu ile içeriği merak ve ilgi uyandıran eğlence, reklam, duygu sömürüsü, yardım, bankacılık, toplum mühendisliği gibi davetsiz spam nitelikte mailler gönderilmektedir. Zararlı ve gizli kod taşıyan bu e-postalar kullanıcının adres defteri, İnternet bankacılığı kimlik bilgileri, kullanıcı girişi yapılan siteler, mesajlaşma içeriği gibi hassas bilgileri ele geçirmektedirler. Kullanıcılar bu saldırılara karşı mücadele verirken bilgi kaynaklarını, değerli olan zamanlarını ve paralarını kayıp etmektedirler.

Bu çalışma dünyada 1 milyardan fazla internet kullanıcısının temel sorunu haline gelen istenilmeyen e-postaların önlenmesine yönelik yapılmıştır. Ağ üzerinde yayılan spam saldırıları e-posta trafiğinin yaklaşık %85'ini, oluşturmaktadır. Bunun ise %95'i zararlı yazılımlardır. (IDS 2007). Aynı zamanda bilgi güvenliğini tehdit eden virüs, truva atı, solucan, tuş kaydedici ve casus yazılım gibi araçlarla kişisel verilerilere erişmek isteyen hacker kişilerin faydalandığı güvenlik açıkları gözden geçirilmiş, kullanıcı ve sunucu tarafında alınması gereken önlemler incelenmiştir. Açık kaynak kodlu yazılımlarla spam e-postaların ve zararlı eklentilerin filtrelenmesine yönelik çözüm örneklerini de içeren bu çalışma beş bölüm altında toplanmıştır. Uygulamada; hızlı, güvenilebilir, düşük maliyet ve özgün kural tanımlama avantajından dolayı açık kaynak kodlu uygulamalar tercih edilerek bunun üniversitenin spam'le mücadelesine ayrıca katkı sağlayacağı düşünülmüştür.

Bu tez 2007 yılında yapılmış ve 96 sayfadan oluşmaktadır.

Anahtar Kelimeler: Internet güvenliği, zararlı yazılım, anti-spam, açık kaynak kodlu yazılımlar.

ABSTRACT

Master's Thesis, Development of an Anti-Spam Module using Open Source Security Softwares, T.R. Maltepe University, Science Institute, Department of Computer Science.

Data access is no more central or limited with the usage of computer and internet technologies. Data can be stored in distributed locations and accessed over network. With the addition of the facts of e-mail and web based threats, security of data has seriously changed in size and character and become more important.

By the increasing of network users depend on cheapen personel network access, the harmful softwares become more effective on a wider area. This environment gives the malicious people the chance to reach legal users easily. Thus the network has become a field of a technological war including illusive, harmful and negative items. E-mail is the largest and the oldest electronical communication method and it is used for reading, sending, replying and arranging messages and appointment. With the awareness of the continuously growing interactive communication, virus coders and cheaters send spam mails including items of interest and wonder stimulating, entertainment , introduction, emotion exploiting, banking, social engineering, etc. These e-mails including harmful and hidden codes seize users' confidential information like address book, internet banking information, identity information, login information for any site, message content, etc. Legal users lose their confidential information, time and money while trying to protect themselves against these threats.

This jop of work aims to present methods for protecting against spam e-mail messages those has become primary problem of the internet users over 1 billion. Spam attacks form approximately %85 of the e-mail traffic and %95 of these attacks include harmful softwares (IDS 2007). Also security gaps exploited by hackers those want to access confidential information by using tools like virus, trojans, worms, key loggers, spywares, etc and precautions should be taken on the side of the servers and users are examined within this work. This work including solutions for filtering of spam e-mails and malicious attachments by using open source software consists of five sections. It is considered that usage of open source applications due to the advantages of speed, reliability, decreased cost and individual rule setting will help with the struggle against spam e-mails on the network of the university.

The thesis is edited in 2007 and consists of 96 pages.

Keywords: Internet security, harmful software, anti-spam, open source softwares.

TEŞEKKÜR

Bu tez konusunu seçmemde ve araştırmalarımda desteklerini esirgemeyen, tezin biçim ve içerik bakımından her zaman değerli fikir ve tecrübelerine başvurduğum tez danışmanım Sayın Prof.Dr. Mesut Razbonyalı'ya teşekkür ederim.

Sistemin tasarlanması ve programlanması sırasında karşılaşılan sorunların birlikte aşılmasında yardımlarını esirgemeyen çalışma arkadaşlarıma teşekkür ederim.

Maddi-manevi desteklerini ve koşulsuz güvenlerini her zaman hissettiğim sıkıntılarımı değil, benimle tüm hayatı paylaşan sevgili aileme teşekkür ederim.

İÇİNDEKİLER

KISALTMALAR

DoS	(Denial of Service), Hizmet aksatma saldırıları
FTP	(File Transfer Protocol), Dosya iletim protokolü
GNU	(GNU's not UNIX), Unix işletim sistemi
HIT	Bir web sayfasını ziyaret eden kullanıcı sayısını ifade eder
HTML	(Hypertext Mark-Up Language), İleri metin işaretleme dili
HTTP	(HyperText Transfer Protocol), İleri metin aktarma protokolü
IDC	Uluslarası anket ve araştırma merkezi
ISDN	(İntegrated Services Digital Network), Veri iletim Şebekesi
LAN	(Local Area Network), Yerel bilgisayar ağı.
LINK	Web sitelerinin farklı sayfalara geçişine olanak veren bağlantılar
P2P	(Pear to Pear), Eşten eşe
POP3	(PostOffice Protocol 3) Elektronik posta protokolu
SMTP	(Simple Mail Transfer Protocol), Posta iletim protokolü.
SSL	(Secure Socket Layer), Güvenli soket katmanı
TCP/IP	(Transfer Control Protocol), İnternet Protocol, Protokoller kümesi
URL	Uniform Resource Locator
WAN	(Wide Area Network), Geniş bölge ağları
WWW	(World Wide Web), Linkleri birbirine bağlayan geniş bilgisayar ağı

ŞEKİLLER VE TABLOLAR

BÖLUM-1

1 INTERNET VE GÜVENLİK

1.1 Internet Kavramı ve Tarihi Gelişimi

Farklı mekânlardaki bilgisayarlar arasında iletişim fikri, ilk olarak 1960′lı yıllarda ABD Savunma Bakanlığı'nda oluşmuştur. İlk uygulama, NASA içerisinde gerçekleştirilmiştir. Daha sonra NASA'ya mal satan firmalar ile NASA arasında bağlantı sağlanmıştır. Bunun sonucunda firmalar da alt kuruluşları ve mal satın aldıkları işletmeler ile iletişimi sağlamak amacıyla sisteme dahil olmuşlardır. Farklı sistemler arasındaki iletişimi sağlamak amacıyla, 2 Eylül 1969 yılında oluşturulan network, ARPA (U.S. Advanced Research Projects Agency) adını almıştır. 1970′lere gelindiğinde, araştırmacılar yeni ARPANET tekniklerini iletişim protokollerine uyarlayarak tek bir network iletişimine başlamışlardır. Bu protokol NCP yerine kullanılmaya başlanan TCP/IP'dir. ARPANET sonradan kaldırılmıştır fakat TCP/IP protokolü gelişmeye devam etti. Bunun sonucunda Unix kullanan birçok üniversitede TCP/IP desteklenmeye başlanmıştır. 1980′lerin başında farklı TCP/IP protokolleri birleştirmek amacıyla INTERNET geliştirilmiştir.[1]

1965′te MIT'den Leonard Kleinrock ile birlikte Roberts ve Thomas Merrill paket anahtarlama teorisi ile Mass.'taki bir TX-2 bilgisayarı ile California'daki bir Q-32 bilgisayarını düşük hızlı dial-up telefon hattı üzerinden birbirileri ile haberleştirmeyi ilk kez başarmıştır. Bu kurulan ilk geniş-alan(wide-area) bilgisayar ağı olmuştur. İlk ortaya çıkan ARPANET, büyüyerek Internet olmuştur. [2] Internet, pek çok farklı tasarıma sahip birbirinden bağımsız ağların varlığı fikrine dayanır. Bugünkü Internet, açık mimarili ağ adi verilen bir kavrama dayanır. Devlet birimleri, endüstri ve akademik kuruluşlar bu yeni teknolojiye büyük ilgi gösterdiler. Günümüzde sıkça rastladığımız "xxx@maltepe.edu.tr" veya "http://www.maltepe.edu.tr" gibi terimler artık insanların ortak dili olmaya başlamıştır.

Internetin tarihinde toplumsal açıdan teknolojik gelişmenin sağlanması ve büyük bir haberleşme ağının gereksinimi etken olmuştur.

1.1.1 İnternette Yaygın Kullanıma Geçiş

Internet'in kullanımının yaygınlaşması ile birlikte diğer ticari ve idari kurumlar da kendi ağlarını kurmaya başladılar. Örneğin askeri kurumlar, ticari kurumlar, eğitim kurumları ve bireysel kullanıcılarla Internet büyüdü ve yedi kıtada toplam 50.000 ağa, Amerika'da ise

29.000 ağa ulaştı. [2] Internet günümüzde genel olarak Ulusal Bilgi Altyapısı adi verilen yaygın bir bilgi altyapısının protipi durumundadır. Internet'in etkisi sadece bilgisayar haberleşmesinin teknik alanları ile sinirli kalmayıp toplum yasayışına da yansımıştır.

Internet, bilgisayar ve haberleşme dünyasını daha önce hiç görülmedik bir şekilde etkilemiştir. Telgraf, telefon, radyo ve bilgisayarın icadı ile bu hizmetler entegre hale getirilmiştir. Internet, dünya çapında yayınlanan bilgilerin paylaşımı için bir mekanizma ve coğrafi yerlerinden bağımsız olarak bilgisayarları birbirine bağlayan bir ortamdır.

1.1.2 Günümüzdeki İnternet

Internet, ilk ortaya çıkısında zaman paylaşımlı iken daha sonra kişisel bilgisayar, istemci-sunucu, uçtan uca haberleşme ve ağ bilgisayarı gibi yönlere kaydı. Internet, LAN kavramı ortaya çıkmadan önce tasarlandı ancak günümüzdeki yeni teknolojilerle (örneğin ATM ve çerçeve anahtarlamalı servisler) uyum sağlanmıştır.

Internet'in değişim sürecinin bittiğini söylemek mümkün değildir. Internet, ADSL, metro ethernet, telefon ve televizyon, bilgisayarlar gibi teknolojileri kapsayan büyük bir ağdır. Günümüzde ses ve video için gerçek zamanlı transfere izin verecek şekilde gelişmektedir. Bu İnternet üzerinden haberleşmenin her geçen gün daha hızlı bir şekilde gerçekleşmesi demektir. Internet'in geleceği ile ilgili en önemli soru teknolojinin nasıl değişeceği değil, değişim prosesinin nasıl yönetileceğidir. Başlangıçta da söylendiği gibi Internet, bir grup tarafından tasarlandı başka gruplar ortaya çıktıkça bu orijinal tasarıma eklemeler oldu.

İnternet, gelişmesine paralel olarak bir çok güvenlik sorununu da beraberinde getirmiştir. Özellikle online alışveriş yapılan sitelerde, müşterilerin güvenli diye düşündükleri bir çok web sitesinden bile kullanıcıların kredi kartı numarasından ev adresine kadar her türlü bilgisi ele geçirilebilmektedir. Ayrıca yine İnternet üzerinden hızla yayılan virüsler de bir bilgisayarın baş düşmanlarındandır. İnternet ortamında kimse %100 güvende değildir. Fakat bu tehlikelere karşı önlemler alırsak art niyetli kişilerin işlerini zorlaştırmış oluruz. Antivirüs, anti-spam programları, firewall kullanmanın yanı sıra mecbur kalmadıkça online alışverişler yapmamak. İnternet ortamında gerekmediği sürece hakkımızda doğru bilgi vermemek büyük ölçüde bizi güvende tutacaktır.

1.1.3 Gelecekteki İnternet Beklentisi

Dünyada cep telefonları PC'lerden 3 kat fazla ve büyüme hızı PC'ye göre büyüme 2 kat daha hızlı artış göstermektedir. Cep telefonlardan internete erişebilenlerin sayısı her geçen

gün artmaktadır. Dünya Bankası, dünya nüfusunun 2/3'ünden fazlasının en az bir cep telefonu şebekesinin kapsama alanı içinde yer aldığını bildirmiştir.

Kablosuz telefon piyasasında mobil cihazların fonksiyonlarındaki internet uygulamalarını da kapsayan genişlemenin insanları yeni teknolojileri kullanmaya yöneltmiştir. Bununla birlikte insanların dijitalleşmeye bu derecede bağımlı hale gelmesi, artık bir şeyleri ezberlemez veya hatırlayamaz bazı şeyleri nasıl yapacakları konusunda arama motorlarını kullanmaları, insan hafıza ve hatırlama yeteneğini de olumsuz yönde etkilemektedir.

Bundan 20 yıl öncesine kadar pek bilinmeyen, 10 yıl kadar önce de ülkemizde kullanılabilir hale gelen bu ortamın geleceği ne olacak? O kadar çok yere girdi ki içerik olduğu taktirde(video kayıtları), yeni bir lokal televizyon kanalının 15 dakikada tüm dünyada yayınlanabilir hale gelmektedir. Telefon konuşmaları analog olmaktan çıkıp IP tabanlı dijital bir yapıya kavuşmuştur. Günlükler internette, radyo, televizyon, film, müzik, arabada giderken bulunduğunuz yer vs. Gelecekte "İnternete girmek" veya "İnternete bağlanmak" gibi bir şey kullanmayacağız çünkü internetin dışı diye bir şey olmayacak. Böyle bakınca "İnternet diye birşey olmayacak." gibi geliyor. Yeni nesil internet olarak nitelenen İnternet II konsorsiyumu yaklaşık 200 üniversite, teknoloji endüstrisi kurumu ve kamu kuruluşunun ortak çabalarıyla geliştirilme aşamasındadır. İnternette en hızlı veri aktarımı İnternet II üzerinde 11 bin kilometrelik bir mesafede ortalama 6.25 gigabyte/saniyelik veri aktarım hızına ulaşmıştır.[3]

ADSL (Asimetrik Sayısal Abone Hattı) Asymmetric Digital Subscriber Line sözcüklerinin baş harflerinden oluşan ADSL, mevcut telefonlar için kullanılan bakır teller üzerinden yüksek hızlı veri, ses ve görüntü iletişimini aynı anda sağlayabilen bir modem teknolojisidir. ADSL ile yüksek hızda kesintisiz internet erişimi, hem de aynı hat üzerinden aynı anda telefonla konuşma imkanına sahiptir. [4]

1.2 Internetin Yaşantımızdaki Yeri

Özellikle yukarıda belirtilen ADSL teknolojisi ile birlikte ülkemizde bireysel kullanımda büyük bir artış sağlanmıştır. Fiyat açısından da her geçen yıl daha da uygun hale gelmektedir. Yerel ya da uluslararası her türlü kullanım ve erişime açıktır. Bağlantı için özel yazılım veya donanım için fazla bir masraf gerektirmemektedir. Basit bir network olmamakta, buna karşın farklı network gruplarının birleşimi olmaktadır. Sadece akademisyenler, işadamları veya askeri amaçlı değil, özel ya da ticari amaçlarla da yoğun

olarak kullanılmaktadır. Tablo 1.2'de elde edilen verilere göre ülkemizde de bilgisayar sahibi olanların yarıdan fazlası interneti bir ihtiyaç olarak göremek ve kullanmaktadır.

Yıl	Bilgisayar Sayısı x1000)	İnternet Abonesix1000
2000	2.450	1.550
2001	3.600	2.751
2002	4.760	4.360
2003	5.800	5.410
2004	7.000	6.900
2005	9.000	8.500

Tablo 1.2 Türkiye'de 2000-2005 Yılları Arası Bilgisayar ve İnternet Sayısı

Yapılan araştırmada Türkiye, 30 ülke arasında internet kullanıcı sayısı en hızlı artan ülke olarak gösterilmiştir. Ayrıca, Türkiye'de internet kullanımının % 19 olduğu belirtilmiştir.

Kısaca İnterneti içinde bulunduğumuz yüzyılın en önemli buluşlarından biri olarak niteleyebiliriz. Her türlü bilgiye çok kısa bir sürede ulaşılmasını sağlayan bu sanal ortam bu özelliğinin yanında insanların günlük hayattaki işlerini de büyük ölçüde kolaylaştırmıştır. Bankalarda uzun kuyruklar beklemek yerine bilgisayar üzerinde bir kaç tıklamayla işimizi halletmiş olmak bu konuyla ilgili klasikleşmiş fakat çarpıcı bir örnektir. Bunun dışında insanların bireysel yetenekleriyle tasarladıkları web siteleri hem bir paylaşım ortamı sunmuş hem de insanların bu konuda becerilerini sergiledikleri ve kimi zaman ticari amaçlarla bu işi profesyonelliğe döktükleri uğraşı alanı olmuştur. Yine aynı şekilde bu yöntemlerle binlerce km uzaktaki bir insan eğitimini bu kanaldan alabilmektedir. Her türlü online haberleşme, tanıtım, reklam, duyuru, elektronik posta, dosya paylaşımı ve iletimi ile yoğun bir kargo görevini de üslenmiştir. İnternetin sağladıkları olanakları sınırlamak mümkün değildir. İnternet adlı teknolojiye bakış açımız, hangi amaçla, ne kadar verimlilikle yararlanabildiğimiz önemlidir. Diğer teknolojilerde de olduğu gibi güvenliği ön planda tutarak dolandırıcıların ağına düşmemek şartıyla İnternet doğru şekilde kullanıldığı sürece yarar sağlar.

1.3 E-posta Devrimi

Yüzyıllardır insanlar haberleşmelerini kağıt postalar aracılığı ile yaptılar. Elektronik posta (e-posta), günümüzde uzak ara internetin en popüler uygulaması. internet'le uğraşan hiç kimse "e-posta kullanmıyorum" diyemeyeceği gibi, bugün internet'ten bir haber olan bir çok insan bile e-postadan haberdar. Ülkemizde yaklaşık 15 senelik geçmişi olan e-postanın aslında yaklaşık 40 senelik bir geçmişi var. 1971 yılında

BBN'den Ray Tomlinson adındaki bir mühendis, ARPANET üzerinden insanların birbirleriyle iletişim kurmalarını sağlayan "SNDMSG" adı verilen bir proje geliştirdi. Proje insanların birbirlerine düz yazı mesajları göndermeleri ve bu mesajların elektronik posta kutularında, okunana kadar saklanmasını sağlayacak gelen mesajın, bir önceki mesajın sonuna eklenmesi ile oluşturulan ve önceki mesajların silinmesine imkan tanımayan bir düz yazı sayfası şeklinde ilk uygulama oldu. Bundan sonra Ray Tomlinson "SNDMSG" projesini bir adım ileriye götürecek olan "CYPNET" projesine önderlik etti. CYPNET insanların posta kutularına düz yazı mesajlar göndermek ile birlikte bilgisayar dosyaları da göndermeye olanak tanıyordu. Bu uygulama ile birlikte e-posta da popüler olmaya başlamıştır. Ray Tomlinson ayrıca bugün posta adreslerini tanımlamakta kullanılan "@" sembolünü de e-posta adreslerine entegre etmişti. [5]Dosya gönderiminin de mümkün kılınması ile birlikte e-posta kullanımı hızla popüler oldu. Hatta e-Postanın icadından iki yıl sonra yapılan bir araştırma, ARPANET'deki internet trafiğinin %75'ini epostaların oluşturduğunu belirtiyordu. İnternet'in yavaş yavaş halka açılmasıyla birlikte tabii ki e-posta da kitlelerle buluşuyordu. 1988 yılında sadece e-posta işleri ile ilgili ilk bilgisayar programı "Eurora" yazıldı. Illinois Üniversitesi'nde çalışan Steve Dorner'ın yazdığı tarihteki ilk grafik arabirimli e-posta programı 1994 yılında başka bir şirkete satılana kadar ücretsiz olarak halka sunuldu. Microsoft'un ve Netscape'in internet gezgini programları ile birlikte sağladıkları e-posta programları giderek 1995 yılında Hintli bir bilgisayar programcısı olan Sabeer Bhatia, internet gezginini kullanarak ulaşılabilecek ilk posta servisi "Hotmail"'i kullanıcılara sundu. Daha sonraları Yahoo ve G-Mail gibi bir çok internet tabanlı posta servisi veren şirket hizmet vermeye başladı. Bugün internet'te posta servisi alanların %30'luk bölümü sadece internet tabanlı posta hizmeti kullanırken, bir milyardan fazla posta adresinin bu servisler tarafından kullanıcılara sağlandığı düşünülüyor. Tarih boyunca insanoğlu hiçbir iletişim aracından bu kadar hızlı, isabetli ve güvenilir ve bedava yararlanamamıştı. Bunun sonucunda ilk e-mektubun atılmasından günümüze e-posta bütün iletişim şeklimizi değiştirdi. 2005 yılı itibari ile tüm dünyada insanlar günde 35 milyon ileti alıyorlar veya gönderiyorlar. Dünya çapında 651 milyon e-posta kullanıcısı varken, 690 milyon e-posta kutusu hizmet görüyor. Geçtiğimiz yıl 180 milyon dolarlık e-posta yazılımları pazarı oluştu. Fakat böyle büyük bir veri akışının ancak %15'lik bir bölümü gerçekten bilgi aktarımına gidiyor. Geriye kalan %85'lik bir bölüm ise e-posta kullanıcılarının en büyük dertleri olan "SPAM" trafiğinde.

Kullanıcılarının %80'ini 13 ile 21 yaş arasındaki gençlerin oluşturduğu bu programı şirketler fark etmekte gecikmediler. Microsoft Messenger ve Yahoo Messenger gibi uygulamalar pazarı genişletti. İnternet servis sağlayıcıların kullanıcılara sundukları e-posta adresleri dışında kullanıcılar internet tabanlı posta servislerine de ücretsiz olarak sahip olabiliyor. Ücretsiz olarak spam filitesi ve virüs koruması olup posta hizmeti veren bazı servisler; www.emailaddresses.com, www.gmail.com, www.hotmail.com.tr (Türkçe), www.mail.com, www.mynet.com (Türkçe), www.netscape.com, www.yahoo.com.

1.4 İstenilmeyen Elektronik İletiler

1.4.1 Spam Tanımı

Spam iletinin tanımı uzun süredir tartışılan bir konudur ve "E-posta ile Pazarlama" endüstrisinin de yaygınlaşması ile beraber ortak bir tanım üzerinde hukukçular, pazarlamacılar, Internet servis sağlayıcıları ve kullanıcılar olarak uzlaşmak hayli zor görünmekte bu yüzden hukuki yaptırımları beraberinde getirmek üzere düzenlenmesine çalışılan kanunlar gecikmekte ya da işlevselliğini yitirmiş şekilde çıkmaktadırlar. İnternet üzerinde aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere, zorlayıcı nitelikte gönderilmesi "istenmeyen elektronik iletiler kısaca ***spam*** olarak adlandırılır. Spam iletilerinin masrafı düşük olduğundan iletiler gönderilirken bir hedef kitle aranmaz ve bu tür mail'leri almak istemeyen binlerce kişi rahatsız edilir[2]. Spam gönderici açısından çok küçük bir harcama ile gerçekleştirilebilirken mali yük mesajın alıcı veya taşıyıcı, servis sağlayıcı kurum tarafından karşılanmak zorunda kalınır. Yapılan istatistiklerde spam problemi her geçen gün daha kötüye gitmektedir.

İnternet kullanıcıları üzerindeki etkileri incelendiğinde iki tip Spam vardır. Email aracılığıyla gönderilen spam doğrudan gönderilen mesajlarla, bireysel kullanıcıları hedef alır. Email spam listeleri genellikle gönderilerinin taranması, tartışma gruplarının üye listelerinin çalınması veya web üzerinden adres aramalarıyla oluşturulur. Email tipindeki spam gönderileri tipik olarak alan kullanıcının masraf yapmasına sebep olur. Email erişimi için süreye bağlı telefon parası ödeyen her kullanıcı için bir bedel ortaya çıkması kaçınılmazdır. Bununda ötesinde, spam maillerinin taşınmasının servis sağlayıcılar ve diğer on-line servisler üzerinde oluşturduğu mali yük de doğrudan abonelere yansıyacaktır.

E-posta yolu ile spam türlerinden ticari içerikli olan UCE (Unsolicited Commercial e-mail- Talep Edilmemiş Ticari e-posta) istemediğiniz halde size gönderilen bir ürünü yada hizmeti tanıtıcı elektronik posta iletileridir. [6]

İçeriğinin mutlaka ticari olması gerekmeyen UBE (Unsolicited Bulk e-mail Talep Edilmemiş Kitlesel e-posta), aynı anda yüzbinlerce e-posta hesabına gönderilen e-posta iletileridir. Bu iletiler ticari içerikli olabileceği gibi politik bir görüşün propagandasını yapmak yada bir konu hakkında kamuoyu oluşturmak amacı ile gönderilen e-posta iletileri de olabilir. Spam hakkında önemli bir nokta, bir iletinin spam olarak nitelendirmek için kullanılacak ölçütün iletinin içeriği ile hiç alakalı olmamasıdır. Herkesin üzerinde hemfikir olduğu, önemli bir toplumsal duyarlılığa sahip bir konu hakkında görüş bildirmek için kitlesel olarak gönderilen bir iletide aslında spam olarak nitelendirilebilir.

Bir diğer sık rastlanılan e-posta spam tipi ise MMF (Make Money Fast – Kolay Para Kazanın) iletileri; zincir iletiler yada piramit benzeri pazarlama yapıları ile ilgili gelen iletilerdir. Piramitin en üstündeki isme para gönderip listenin altına kendinizi eklediğinizde para kazanmaya başlayacağınıza ilişkin iletiler bu tip spame örnek olarak verilebilir.

Email türündeki spam'in rahatsız edici bir tipi ise, iletinin tartışma listelerine gönderilmesi durumudur. Bir çok tartışma listesinde, kimi işlemler sadece liste üyeleri tarafından gerçekleştirilebildiğinden, spam göndericileri, mümkün olduğu kadar çok listeye üye olmaya çalışarak, liste üyelerinin adreslerini temin ederler.

Diğer bir Spam tipi ise, iptaledilebilir (cancellable) mesajları aracılığı ile yapılan spamdir. 20 veya daha fazla haber öbeğine aynı anda gönderilen bir ileti spam kapsamında incelenir. Usenet kullanıcıları açısından bu kadar çok sayıda haber öbeğine gönderilen bir iletinin genellikle öbeklerin çoğu, hatta hepsi açısından konu dışı kaldığı tesbit edilmiştir. Bu tür spam, sıklıkla haber öbeklerini okuyan ancak çok ender veya hiç gönderi yapmadıklarından email adresleri elde edilemeyen kullanıcı grubunu hedefler. Usernet spamleri haber öbeklerini reklamlar veya ilgisiz iletilerle doldurarak kullanıcı açısından faydasız ve kullanılması zor hale getirir.

IBM şirketi Internet Security Systems (ISS) Ar-Ge ve istihbarat birimi **X-Force**'un 2006 yılında yaptığı araştırma raporlarına göre bazı tespitler;

- 2006'da, ISS'in 2005 raporuna göre spam artışı % 100.

- En fazla spam kaynaklanan ülkeler ABD, İspanya ve Fransa.
- Spam dili olarak İngilizce hala önde olmakla beraber, hemen ardından gelen Almanca ikinci en popular spam dili. (spam mesajların açılmasını ve okunmasını sağlamak için saldırganlar olabildiğince farklı diller kullanıyor)
- 2006'nın en popular spam konu başlığı: "Re:hi."
- En fazla yemleme e-postası Güney Kore'den kaynaklanıyor.
- 2006'nın en büyük tehdit kategorisini, "downloaders" adı verilen ve daha sonra çok daha zararlı yüklemelerin kapısını açmak üzere kendini bilgisayara yükleyen düşük tehdit etkili programlar oluşturdu.
- 2006'da en fazla açık Haziran ayında yaşanmıştır.

X-Force, 2007'de **görüntülü spam** tekniklerinin daha sofistike hale geleceğini öngörüyor. 2006'da az sayıda formlarına rastlanan görüntülü spam'e karşı geliştirilen koruma mekanizmalarını aşacak daha etkin görüntülü bazlı spam şekillerinin ortaya çıkması öngörülmektedir. [7]

1.4.2 Spam ile savaşan kuruluşlar

Spam ile savaşan belli başlı bağımsız organizasyonlar olarak aşağıdakiler verilebilir:

- **TASO** - "***Türk Anti-Spam Organizasyonu***", 1999 yılında kurulmuş sanal bir çalışma grubudur. Organizasyonun hedefi kamuoyunu bilinçlendirmek ve Türkiye'de spam ile mücadele edebilmek için teknolojik çözümleri tartışmak ve oluşturmaktır. Grup çalışmalarını http://www.spam.org.tr web sitesinden ve bir tartışma listesinden yürütmektedir.[8]
- **CAUCE** (The Coalition Against Unsolicited Commercial Email) dünya çapında spam ile savaşan bir bağımsız organizasyondur (http://www.cauce.org). Bu organizasyon Avrupa, Kanada ve Hindistan'daki alt kuruluşlarla desteklenmektedir.
- **SPAMCON** Foundation (http://www.spamcon.org/)
- **FREE** (www.spamfree.org)

1.4.3 Hukuksal Boyut

CAUCE organizasyonlarının düzenlediği anketler ve çalışmalara göre kullanıcılar spam mesajlarının bir pazarlama aracı olarak yaygın kullanımını kontrol altına alacak yasalar talep etmektedir. Avrupa Birliği, ***Opt-in Politikası***'nı kabul etmiş ve kullanıcının daha önceden rızası olmadan ticari mail'lerin gönderilmesine EEA (European Economic Area) içinde izin verilmeyeceğini belirtmiştir[4]. ***Opt-in Politikası***, kullanıcıların ihtiyaç duydukları alışveriş ve pazarlama bilgisini talep etme fırsatını sağlamakta ve böylece

pazarlamacılar da hedefledikleri kitleye ulaşmaktadırlar. Böylece İnternet Servis sağlayıcıları da hızlı, efektif ve güvenli elektronik posta akışını sağlayabilme imkanına ulaşmaktadırlar.

Genel anlamda Bilgi Güvenliği, özelinde Bilişim Güvenliği, ülkemizde de önemli konulardan biri haline gelmiştir. Henüz işin başındayız ve başında olduğumuz için de temel kavramların anlaşılması ve oturtulması, sağlıklı bir güvenliğin sağlanabilmesi için önemli. Bu temel kavramlar bu belgenin konusunu oluşturuyor.

Kısa vadeli çözümler kullanıldığında bilgi sistemlerimize antivirüs yazılımı olduğu halde virüs bulaştığına, ateşduvarı olduğu halde izinsiz erişim sağlandığına, e-mektuplarımızın şifreli gönderdiğimiz halde saldırganlar tarafından okunduğuna, dosyalarımızın anlayamadığımız yollarla kaybolduğuna, yine anlayamadığımız bir sebepten herhangi bir sunucu programın çalışmadığına, hatta bilgisayarımızın bir saldırgan tarafından bizden daha fazla kullanıldığı durumlarla karşılaşılmaktadır.

1.4.4 Açık Kaynak Kodlu Yazılım Desteği

Kurumsal yazılım geliştirme pazarında açık kodlu araçlar ciddi pazar paylana ulaşmıştır. Bu kazanım sadece ücretsiz olmalarından dolayı kaynaklanmıyor. Bu ürünler hem kullanım kolaylığı, hem de ürünle ilgili kaynak fazlalığı açısından ciddi gelişme gösterdiler ve pazarda yerlerini aldılar. Açık kodlu ürünlerin kodlarındaki güvenlik hataları kodu inceleyen üniversiteler, güvenlik şirketleri, vs. tarafından tesbit edilip duyuruluyor ve hemen hatanın temizlendiği sürüm yayınlanıyor. Dolayısıyla güvenlik konusunda açık kodlu ürünler, diğer ticari ürünlere göre avantajlı durumda.

İşletim sistemi, uygulama sunucusu, veritabanı, uygulama geliştirme aracı, vs. gibi paket olarak satılabilen ürünlerde, açık kodlu ve ücretsiz ürünlerin kullanımı daha da yaygın hale gelecektir. Kurumsal projelerde sıkça kullanılan uygulama sunucuları, kullanım ve bakım kolaylığı gibi konularda daha çok tercih edilir duruma gelmiştir.

1.4. Döküman ve Kaynak Paylaşımı

Kullanıcılar için değerli, saldırganlar için ise birer hedef olan yazılım, donanım ve veriye saldırıya karşı savunmada olmak gerekmektedir. Genel olarak "paylaşım ve güvenlik" korunmakta olan bilginin gizliliği, bütünlüğü, ve ulaşılabilirliği olarak ifade edilebilir. Gizlilik bilgiye sadece izin verilen kişilerin izin verilen yollarla erişimi anlamındadır. Burdaki erişim, okumaya yönelik bir erişimdir (örn: kopyalama, yazdırma, bilgi için

fotokopi). Yetkisiz kişilerin bir bilginin varlığının bilgisine dahi erişimleri bir güvenlik ihlalidir. Bu amacı ihlal etmeye yönelik saldırı türü ve paylaşım izinsiz erişimdir.

Bilginin bütün oluşu herşeyden önce doğru ve kesin oluşu, şüphe uyandırmayan bir durumda korunmasıdır. Bilgi aynı zamanda değiştirilemez olmalı, sadece izin verilen yetkililerce izin verilen yollarla değiştirilebilmelidir. Bilginin bütünlüğünü ihlale yönelik saldırı türleri engelleme veya zarar verme, değişiklik yapma, ve üretim olabilir.

Bilginin ulaşılabilir oluşu, en az bilginin gizlilik ve bütünlük amaçları kadar önemli bir amaçtır. Ulaşılabilirlik demek, bilginin yetkili kişilerce erişilebilir olmasının yanında kullanılabilir de olması demektir. Aynı zamanda bilgi kullanıcılar tarafından zamanında ulaşılabilmeli, ve ulaşım sırasındaki kaynak paylaşımı izin verilen şekilde olmalıdır. İnternet üzerinden saldırı türü engelleme veya değişiklik yapma şeklinde olabilir.

1.4.1 Veri Aktarım Güvenliği

Veri aktarım güvenliği, verinin bulunduğu noktadan iletileceği noktaya kadar olan aradaki tüm erişim durumları gözden geçirilmelidir. Verilerin depolanma alanı, hafıza, internet hattı, pc geçici alanı gibi alanların tamamı veri güvenliği için oldukça önemlidir.

Amaçlanan veri güvenliğin sağlanması ancak arada kullanılan yazılım ve erişim hattının yanı sıra insan faktöründen kaynaklanan güvenlik açıklarının "zayıflıklar"ın da en aza indirgenmesi ile mümkündür. Bunların neler olabileceği ile ilgili şu örnekler verilebilir:

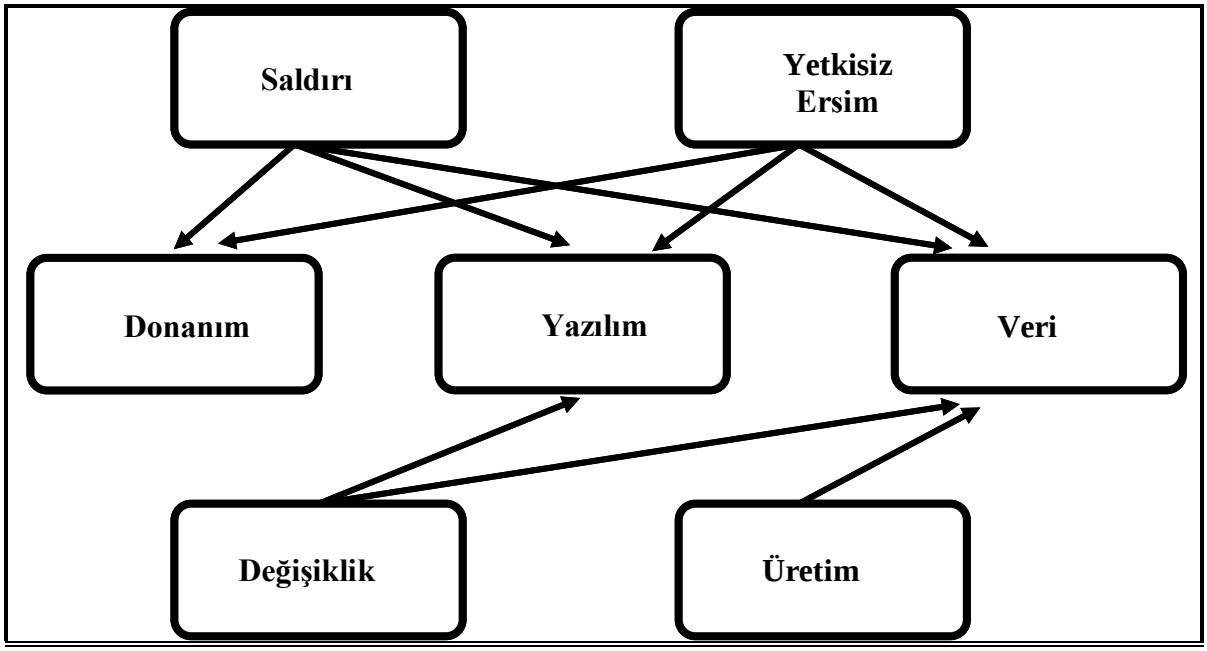
- Ağ yapılandırmasındaki mimari yanlışlar
- Yanlış transaction kullanımı
- SQL açıklıkları
- Uyarı hatalarının ele alınmaması
- İstisnaların ele alınmaması
- Ağ trafiğine sonsuz güven duyma
- URL bazlı veri girdi risk kontrolü
- Uygunsuz SSL kullanımı
- Zayıf şifre yapıları
- Kriptografi için yetersiz algoritma
- Güvensiz veri saklama
- Veri sızıntısı
- Uygunsuz dosya erişimi (veri kaybı)
- Yetkilendirilmemiş kullanıcı değişimleri

BOLUM-2

2 E-POSTA GÜVENLİĞİ VE TEHDİTLER

Günümüzde bilgisayar uygulamasında gereksinim duyulan her türlü sayısal iletişim ihtiyacının karşılanması bilgisayar ağlarından beklenen hizmet türleri ve hizmet kalitesi artmaktadır. Bunu karşılamak amacıyla da kurumlar, firmalar hem kendi alt yapılarını güçlendirmekte hemde önceden var olan internet gibi tüm dünyaya yayılmış global ağlardan olabildiğince yararlanmaktadır. Internetin genişlemesi ile beraber ağ uygulaması, ağ yönetimi ve ağ güvenliği büyük önem kazanmış ve ağın güvenilir biçimde çalıştırılması anahtar konumuna gelmiştir. Ancak tedbir sadece firewall`la sınırlı olmamalıdır.

Sistem kullanıcıları için değerli olan ve saldırganlar içinde hedef anlamına gelen yazılım, donanım ve verinin maruz kalabileceği saldırı ilişkileri şu şekilde özetlenebilir.



Şekil 2 Saldırı tipleri arasındaki ilişki

Şekil 2'de görüldüğü gibi engelleme ve izinsiz erişim her üç sisteme de, değişiklik yapma sadece yazılım ve veriye, üretim ise sadece veriye yönelik bir saldırıdır. Değişiklik yapma ilk bakışta donanıma da yöneltilebilecek bir saldırı gibi görünse de, burdaki değişiklikten kasıt, fiziksel bir parçanın değiştirilmesi değil, daha çok çalışmanın veya içeriğin beklenenden ayırt edilebilen veya edilemeyen şekil farklı olmasıdır.

Donanımın maruz kalabileceği çalınma, parçalama, kırma, bozma gibi önceden planlanarak yapılan eylem şeklinde yada ihmal ve umursamazlık sonucu ortaya çıkan

kazalar, yıldırım düşmesi, deprem ve sel gibi doğal afetler, veya yangın gibi doğal olmayan bir afet sonucu da olabilir.

Yazılımın maruz kalabileceği saldırılar arasında, **silinme** baş sırayı almaktadır. Kullandığınız işletim sisteminin yönetici yetkilerindeki kullanıcısını (örn: Windows için Administrator, Unix için root kullanıcısı), sadece ihtiyacınız olduğunda kullanmalı, diğer zamanlardaki olağan işlerinizi, normal yetkilerde, yani yetkileri kısıtlandırılmış olan bir kullanıcı ile gerçekleştirilmelisiniz.

Yazılımın tek zayıflığı silinebilir olması değildir. Yazılım üzerinde aynı zamanda **değişiklik** de yapılabilir. Derlenmiş bir program üzerinde değişiklik yapmak metin bir dosya üzerinde değişiklik yapmaktan çok daha zor ve özel bir bilgi ve özel programlar kullanmayı gerektirir. Bununla birlikte, herhangi bir programın üzerinde değişiklik yapacak programlar yazılabilir. Belki de en çok kişinin aşina olduğu saldırı türü, aslında yazılıma yönelik değişiklik yapma saldırısıdır, virüsler ve truva atları bu amaçla hazırlanan programlardan başka bir şey değildir aslında. Virüsler belli bir amaca yönelik bu saldırıyı yaparlar, ve bu amaçlar çok değişik olabilir. Sadece bir ileti görüntüleyen virüsler de vardır, bütün bilgisayardaki dosyaları ulaşılmaz hale getiren virüsler de. Truva atları, genelde bulaştığı bir bilgisayarda, saldırgan için sınırsız erişim olanağı sağlar (bazı durumlarda bilgisayarın başında normal yollarla yapılamayacak işlemlerin bile yapılabilmesine olanak tanır). Truva atlarının varlığını anlamak virüslerden farklı olarak kolay olmayabilir, çünkü belirtileri tamamen truva atını koyan kişinin yapacaklarına bağlıdır, yine virüslerden farklı olarak truva atları kendi başlarına (genelde) yayılmazlar.

Virüs ve truva atlarının yanında, yazılıma konmuş arka kapılar olabilir. Bunlar programı yazan kişi tarafından oluşturulmuş, ve programın erişim sınırlamalarının ötesine geçebilir. Hatta sadece bilgi sızdırma amacıyla da yazılımda izinsiz değişiklik yapmak istenebilir.

Yazılım ve donanımın olduğu kadar, verinin de açıkları, yani zayıf yönleri vardır. Sahte veri üretimi ya da özgün verinin kopyalanarak amaca yönelik değişiklik yapılması, yani veri taklidi de veriye yönelebilecek saldırı türleri arasındadır.[9]

2.1 Sistem Açıkları

İnternet herkese açık, bilginin rahatça paylaşılabildiği bir ortamdır. Bu ortamda iyi niyetli kullanıcıların yanı sıra, zarar vermek isteyen, kötü niyetli kişiler de bulunabilmektedir.

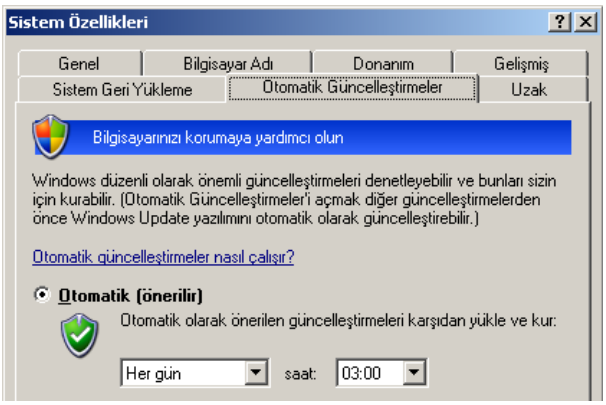
İnternet üzerinden yapılan saldırılar genellikle bir e-posta ile gelen veya sohbet odalarından gönderilen programlarla yapılmaktadır. Bu programlar genellikle bilgisayarın görev listesine (task list/manager) bakıldığında görünmezler. İstem dışında fonksiyonlar gerçekleştiren programlar Truva Atı (Trojan Horse) olarak adlandırılır.

Ayrıca İnternette kişisel bazlı saldırılar yoğun olarak görülmekte olup, bilgisayarlardaki dosyalar, şifreler, klavyeden basılan tuşların yakalanması gibi bilgiler bir başkası tarafından elde edilebilmekte, bilgisayar bir başkası tarafından uzaktan kontrol edilebilmektedir. Bu nedenle, internette bulunabilecek risk faktörlerini bilmek tehlikelere karşı tedbirli olmak gerekir. Anti-virüs yazılımları, bilgisayar sistemini, tuş vuruşlarını kaydedip internet üzerinden bilgi aktaran trojan dahil olmak üzere, virüslerden korur. [10]

İnternet erişimi olan kişisel bilgisayarların sistem açıklarından dolayı karşılaşacağı olası tehlikeleri aşağıdaki başlıklar altında incelemek mümkündür.

2.1.1 İşletim Sistemi Açıkları

Her işletim sisteminde mutlaka açık kodlar vardır. Üretici firma bu açıkları fark ettiğinde kendi web sitesinde yama ve güncelleme dosyaları yayınlar. Microsoft Windows işletim sisteminin açıklarını kapatmak için http://windowsupdate.microsoft.com web sitesinde yayınlanmaktadır. Hackerların en son yayınlanan yama ve güncellemeleri takip ederek güncel olmayan bilgisayarlara saldırdıkları unutulmamalı ve bu nedenle "Otomatik Güncellemeler" mutlaka etkin olmalıdır. Otomatik güncelleştirmeleri etkinleştirmek için *Denetim Masası => Sistem Özellikleri => Otomatik Güncelleştirmeler* yolu izlenmelidir (Şekil–2.1.1). Ayrıca işletim sistemi bilgisayara ilk defa yükleneceği zaman mutlaka en son güncellemeleri ve yamaları içeren yazılımın bulunduğu CD ile yüklenmelidir.[11]



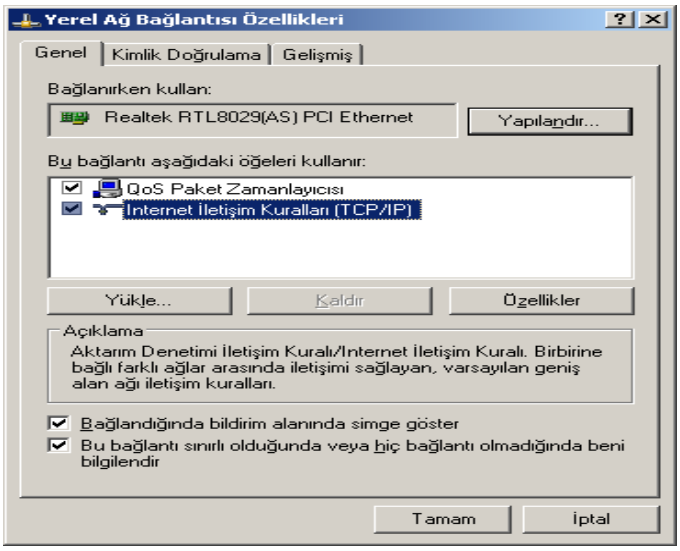
Şekil 2.1.1 Otomatik Güncelleştirmeler

2.1.2 Kullanıcı Hesap Açıkları

İşletim sistemindeki gereksiz bütün kullanıcı hesapları silinmelidir. Yeni ve sınırlı yetkilere sahip olan bir kullanıcı tanımlamak ve interneti bu sınırlı kullanıcı hesabı ile kullanmak bizi internet üzerindeki olası zararlı yazılımların bilgisayarımızdaki bazı önemli ayarları değiştirme tehlikesine karşı koruyacaktır. İnternet kullanılacağı zaman yönetici haklarına sahip kullanıcı ile oturum açmaktan kaçınmak her zaman faydalıdır. Hatta risk altındaki bilgisayarlarda yönetici hesabı mutlaka şifrelenmeli ve eğer mümkünse hedef şaşırtmak için sahte administrator hesabı oluşturulmalıdır.

2.1.3. Gereksiz Paylaşımlar, Protokoller Ve Hizmetler

Kişisel bilgisayarımız bir bilgisayar ağının parçası değilse veya dosya ve yazıcı paylaştırma gibi servisler kullanılmıyorsa bu servisler mutlaka kapalı tutulmalıdır. Hatta dosya paylaşımı sürekli yapılmıyor, çok ender olarak kullanılıyor ise bu servisler yine kapalı olmalı sadece ihtiyaç duyulduğunda etkinleştirilip sonra tekrar devre dışı bırakılmalıdır. Kişisel bilgisayarımız herhangi bir bilgisayar ağının parçası değilse ve sadece internete bağlanmak için kullanılıyorsa ihtiyaç duyduğumuz tek protokol TCP/IP protokolüdür. Denetim Masası'ndan Ağ Bağlantıları'nı açıp Yerel Ağ Bağlantısı özelliklerini görüntülediğimizde bağlantının kullandığı öğelerde TCP/IP ve QoS Paket Zamanlayıcısı dışındaki protokollerin bulunması gereksizdir ve güvenlik açıklarına neden olacaktır (Şekil–2.1.3). QoS Paket Zamanlayıcısı protokolü arka planda sistem güncellemeleri için gerekli olup kullanımda olmasında herhangi bir sakınca yoktur.

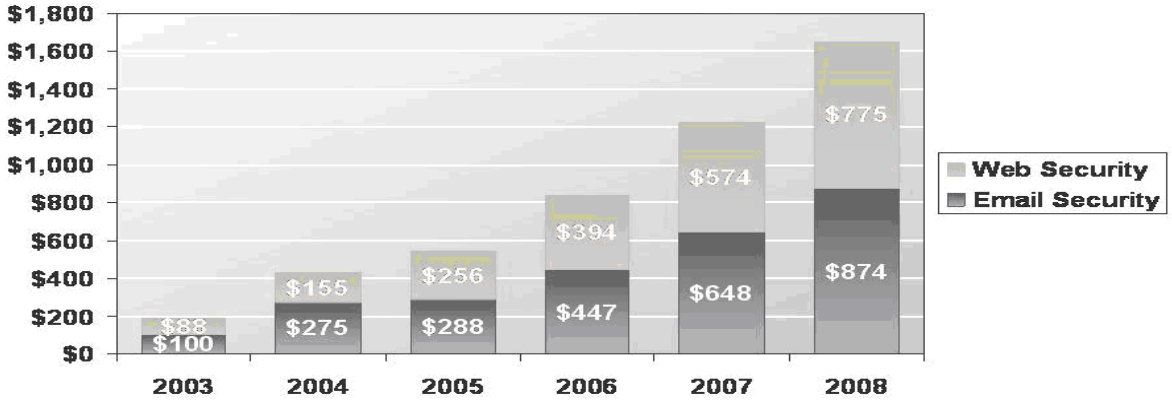


Şekil 2.1.3 Yerel Ağ Bağlantısı Özellikleri

Windows'ta protokollerdeki gibi çalışmasını istemediğimiz hizmetler devre dışı bırakmalı. *Denetim Masası =>Yönetimsel Araçlar => Hizmetler* yolunu izleyerek yapılabilir.

2.1.4 Web Tarayıcılarının Açıkları

2006 yılında gerçekleşen güvenlik açıklarından %87'si WEB protokolleri üzerinden ya da e-posta yolu ile olmuştur. Mydoom, Netsky ve Bagle gibi solucanlar milyarlarca dolarlık zarara yol açarak e-posta ve network hizmetlerinde tıkanmalara yol açmıştır. Spam şeklinde yayılan bu tarz virüsler networklerde arka kapılar oluşturarak milyonlarca kişiye spam göndermiştir. WEB trafiğini güvenliği sağlayan cihazlar yıllık %50'lik bir artışla yayılmaktadır.(600 milyon $ / 2005 yılı – network IPS pazarından daha büyük- IDC**)** Source: IDC August 2004, PM, and Raymond James Reporting[12]



Şekil 2.1.4 Elektronik posta ve web saldırılarının yıllara göre artış dağılımı

Spyware'ler makinanızı harabeye çevirebilir, band genişliğinizi harcar, ve işinize doğruda etki eder, spyware iş sürekliliği için çok ciddi bir tehdittir. Diğer yandan help-desk maliyetlerini artırır, mesela Dell'e gelen destek çağrılarının %25'i spyware kaynaklı olduğu rapor edilmiş.

Microsoft Windows işletim sistemine entegre olarak bilgisayarımızda bulunan ve bugün internet ortamında en çok kullanılan web tarayıcısı olan Microsoft İnternet Explorer ile yine en yaygın olarak kullanılan e-posta istemcisi Outlook Express de hackerların hedefi olmakta ve güvenliğimiz için tehlikeleri içinde barındırmaktadır. Aynı işletim sisteminde olduğu gibi web tarayıcısının ve e-posta istemcisinin de en güncel halde olması çok önemlidir.

2.1.5. Güvensiz yazılım yükleme

Güvensiz yazılımlar illegal olarak kopyalanmış veya internetteki korsan sitelerden indirilmiş yazılımlar olup içlerinde bilgisayarımıza zarar verebilecek virüs, truva atı, tuş

kaydedici ve her türlü casus yazılımı barındırabilen yazılımlardır. Casus yazılımlar ise internette gezdiğimiz web sitelerinin kayıtlarını tutup bizden habersiz başkalarına gönderen, karşımıza istemediğimiz reklam pencerelerinin gelmesini sağlayan, bilgisayarımızdaki şahsi dosyalarımızı başkalarına gönderebilen, bilgisayarımızın performansını düşüren ve internet erişimini gereksiz yere meşgul eden istenmeyen yazılımlardır. Bu tip yazılımlar çoğu zaman sistemimize bizden habersiz olarak yüklenirler. Casus yazılımlardan korunmak için yapılması gerekenler şu şekilde listelenebilir:

- Korsan yazılım kullanmaktan kaçınmak, lisanslı yazılım kullanmak
- Korsan web sitelerinden yazılım indirmemek
- İnternetten yazılım indireceğimiz zaman güvenli web sitelerini kullanmak. Güvenli dosya indirme sitelerinde mutlaka "No ad-aware, no-spyware" gibi uyarılar mevcuttur.
- Sırf bedava olduğu için ne olduğunu bilmediğimiz yazılımları bilgisayara yüklememek. Casus yazılımların çoğu bedava yazılımlarla bilgisayara yüklenir.
- Yazılım yüklerken "son kullanıcı lisans sözleşmesi"ne göz atmak. "Ad-supported" olarak desteklenen yazılımları bilgisayarımıza yüklememek.

Bilgisayarımıza bulaşan casus yazılımları temizlemek için de özel yazılımlar mevcuttur. Anticasus yazılımı Windows Defender (www.microsoft.com/security/spyware/software), Ad-Aware (http://www.lavasoft.com) ve Spybot Search & Destroy (http://www.safer-networking.org/tr/index.html) casus yazılımları tanıyıp temizleme konusunda başarılıdır.

2.1.6 Açıkları Olan Yazılım Kodu

Yazılımlar sistem kaynaklarının izinsiz kullanımını engelleyecek güvenlik özellikleri ile tasarlandıklarından, birçok virüs sistem ya da uygulamalardaki yazılım hatalarını (bug) suistimal ederek yayılırlar. Yazılımlarda çok sayıda hata (bug) bulunduran yazılım geliştirme birçok potansiyel suistimalin de temel kaynağı olacaktır.

Microsoft ve patentli yazılım üreten şirketlerin tercih ettikleri kapalı kaynak yazılım geliştirme süreci birçokları tarafından güvenlik zafiyetinin temel kaynağı olarak görülür. Açık kaynak yazılımlar kullanıcıların uygulama kodlarını incelemesine olanak tanır ve güvenlik problemlerini çözmek için sadece tek bir kuruma bağlı kalmaz.

Diğer taraftan bazıları açık kaynak yazılım geliştirmenin, virüs yazıcılarının kullanabilecekleri potansiyel güvenlik problemlerini açığa çıkardığını ve dolayısıyla

suistimallerin görülme sıklığının artacağını iddia etmekte. Bu kişiler Microsoft gibi popüler kapalı kaynak yazılımların çok fazla kullanıcısı olmasından ötürü süistimal edildiklerini ve yazılımın çokça kullanılması nedeniyle suistimal etkisinin geniş alanlara yayılmasının doğal karşılanması gerektiğini iddia etmekteler.

2.1.7 Virüs saldırılarına karşı açıklar

Bir ağ üzerindeki yazılım sistemlerinin çeşitliliği, virüslerin tahrip ediciciliğini sınırlamaktadır. Microsoft'un masaüstü işletim sistemleri ve ofis yazılımlarında 1990'larda sağladığı üstünlük saldırganlar tarafındanda özel bir ilgiye neden olmuştur. Microsoft yazılımları (özellikle Microsoft Outlook ve Internet Explorer gibi ağ yazılımlar) virüslerin yayılımı karşısında savunmasızdırlar. Microsoft yazılımları, şirketin masaüstü işletim sistemlerindeki nicelik olarak üstünlüğünden ötürü birçok virüs yazıcısının hedefidir ve virüs yazıcılar tarafından suistimal edilen birçok hata (bug) ve açıkları bünyelerinde bulundurduklarından sık sık eleştiri almaktadırlar. Gömülü (entegre) yazılımlar , dosya sistemlerine erişim imkanı tanıyan betik dillerini içerir uygulamalar (örneğin VBScript ve ağ oluşturma uygulamaları) da saldırıya açıktır.

Her ne kadar Windows virüs yazıcılar için en gözde işletim sistemi olsa da bazı virüsler diğer platformlarda da gözlenmektedir. Üçüncü parti yazılımları yürüten herhangi bir işletim sisteminde teorik olarak virüsler çalışabilir. Bazı işletim sistemleri diğerlerine nispeten daha az güvenlidir. Unix temelli işletim sistemleri (ve Windows NT temelli platformalar) kullanıcıların yürütülebilir uygulamaları sadece kendilerine ait sınırlandırılmış alanda çalıştırmalarına izin verirler.

Unix tabanlı işletim sistemlerinden biri olan Mac OS X'de açık suistimali(exploit) oldukça azdır. Apple'in Mac OS Classic olarak bilinen eski işletim sistemlerine yönelik virüslerin sayısı, bilgi kaynaklarına göre değişiklik arz etmekte. Apple sadece 4 , bağımsız kaynaklar ise 63 kadar virüsün işletim sistemine bulaşabileceğini belirtmekte. Unix tabanlı işletim sistemleri güvenlik açıkları yönünden diğer işletim sistemlerine göre daha güçtür.

1997'de Bliss olarak bilinen Linux'a yönelik virüs ortaya çıktığında, önde gelen antivirüs şirketleri Unix benzeri işletim sistemlerinin (Linux) Windows gibi virüslerin esareti altına girebileceği öngörüsünde bulundu.[5] Bliss, Unix sistemlere yönelik tipik bir virustür. Bliss, kullanıcının *kendisini* çalıştırması ile aktif hale gelir ve sadece kullanıcının erişim haklarının olduğu alanları (ya da programları) enfekte eder. Windows kullanıcılarının

aksine birçok Unix kullanıcısı, program yüklemek ve yazılım ayarlarını yapmak gibi durumlar haricinde yönetici hesabıyla oturum açmazlar , dolayısıyla kullanıcı virüsü çalıştırsa bile virüs işletim sistemi dosyalarına bulaşamayacağı için sisteme zarar veremez . Bliss virüsü çok yaygınlaşmadı ve daha çok araştırma merakı aracı olarak kalmıştır.

2.2. Spam Kaynaklı Saldırı Metodları

Bu noktada saldırgan ve saldırı tanımının iyi yapılması gerekiyor. Bir sisteme yöneltilen, güvenlik amaçlarını ihlal etmeye yönelik tüm eylemler, saldırgan ise bu eylemlerde bulunan kişiler anlamında kullanılabilir. Saldırganın bakış açısından hedef olan şeyler, aslında bizler için "bir değer" taşıyan unsurlardır. Bir bilgisayar kullanıcısı için "değerli" olabilecek şeyleri tahmin etmek güç değil: Bilgisayarların temel bileşimleri olan **yazılım, donanım, ve veri**, çoğu sistem kullanıcısı veya yöneticisi için bir değer taşır, bu yüzden de saldırılar bu üç hedefte yoğunlaşır.

Her ne kadar saldırılar çoğunlukla bu üç temel bileşene yöneltilse de, aslında bir saldırının hedefleri arasında, özellikle yedekleme için kullanılan depolama ortamları (örn: disk, CD, tape backup), verinin aktarıldığı ortamlar (örn: kablolu veya kablosuz ağlar) ve hatta zaman zaman kilit görevleri üstlenen insanlar da hedefler arasında yer alabilmektedir. Çoğu zaman göz ardı edilen insan unsuru çok fazla veri kaybına yol açabilmektedir.

2.2.1 En Kolay Giriş Yolu

Herhangi bir saldırgan, korumakta olduğunuz sistemin güvenliğini bozmak için, bulabileceği en kolay yolu deneyecektir. Davetsiz kapıyı çalan spam epostalar kolay yutulur av niteliğindedir. Örneğin evinizi korumak için kapısını son derece güvenli kilitler veya çelik bir zırh ile güçlendirmiştir ancak açık unutulmuş bir pencere saldırgan için daha değerlidir. Yani en kolay yol demek, en belirgin, en çok beklenilen, veya saldırılara karşı en çok önlem alınmış ve güçlendirilmiş yol demek değildir. [13]

2.2.2 Gizlenme

Kullanıcılar tarafından tespit edilmeyi güçleştirmek adına spam türü virüsler bazı aldatmacalar kullanmaktadır. Konak dosyaya bulaşan bir virüs içeriği değiştirmesine rağmen, *son değiştirme* tarihinin özellikle değişmeden kalmasını sağlarlar. Ancak bu yaklaşım ile antivirüs yazılımlarını aldatamazlar.

Virüsler artık ulaştıkları dosyaların büyüklüklerini de değiştirmeden ve dosyaya zarar vermeden bulaşmaktadırlar. Bunu yürütülebilir dosyadaki kullanılmayan alanların üzerine

yazarak gerçekleştirirler. Bu türden virüsler boşluk virüsleri olarak adlandırılırlar . Örneğin bir zamanlar büyük tahribata neden olmuş Chernobyl virüsü taşınabilir yürütülebilir dosyaları etkilemişti çünkü bu tür dosyalarda çok sayıda boşluk bulunmaktadır. 1 KB boyutundaki virüs dosyalara bulaştığında dosya büyüklükleri değişmeyecektir.

Bir kısım virüsler antivirüs programları kendilerini tespit etmeden evvel bazı antivirüs program görevlerini sonlandırarak tespiti engellemeye çalışırlar. Bilgisayarlar ve işletim sistemleri gelişip karmaşıklaştıkca eski tip saklanma yöntemlerinin güncellenmeleri ya da yenileriyle değiştirilmeleri gerektiği açıktır.

2.2.3 Tuş Kaydediciler ve Olta

Tuş kaydediciler genellikle kredi kartı numara ve şifrelerini, internet bankacılığı hesap şifrelerini vb. önemli bilgileri çalmayı amaçlayan, kullanıcıdan gizli olarak arka planda çalışan ve klavye üzerinden basılan her tuş ile farenin hareketlerini anlık olarak kaydeden zararlı yazılımlardır. Tuş kaydedicilerden korunmak için mutlaka sistemimizde bir antivirüs yazılımı ile birde güvenlik duvarı yazılımının aktif korumaları etkin olmalıdır.

Olta yöntemleri ise internet bankacılığı şifresi, e-posta şifresi gibi bilgileri çalmak için oturum açma sayfalarının sahtelerini yapmak ve kullanıcıyı bu sahte sayfaya yönlendirip şifrelerini çalmak için kullanılan yöntemlerdir. Bu tip yöntemlerden korunmak için Windows işletim sisteminde dikkat edilmesi gereken en önemli şey "hosts" dosyasının (C:\WINDOWS\system32\drivers\etc\hosts) bilginiz olmadan değiştirilmesini önlemektir. Örneğin Windows Defender (http://www.microsoft.com/security/spyware/software) Anti-casus yazılımının sistemimizde yüklü ve aktif koruması etkin ise bu dosyada yapılacak olan her türlü değişikliğe karşı kullanıcıyı uyaracaktır. Ayrıca Spyware Blaster adlı yazılım da hosts dosyasını şifreleyerek korumaktadır.

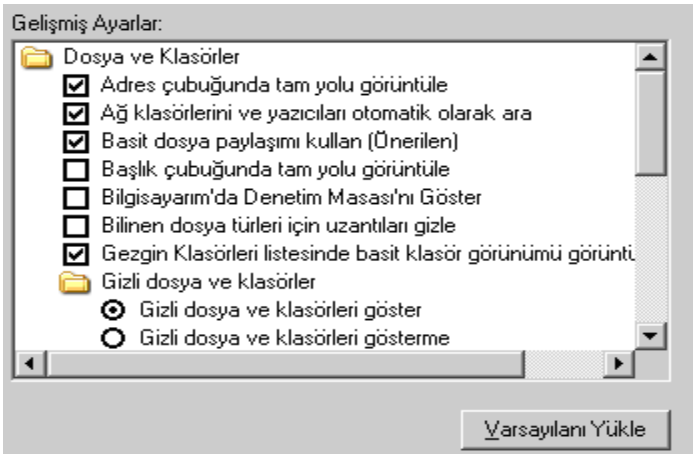
2.2.4. Numara Çeviriciler

Numara çeviriciler özellikle internete çevirmeli bağlantı ile bağlanan kullanıcıların dikkat etmesi gereken zararlı yazılım türüdür. Bu tip yazılımlar internet bağlantısını keserek milletler arası telefon numarası çevirir ve bilgisayarı internete yeniden bağlar[14]. Daha sonra kullanıcı çok yüksek bedelli telefon faturaları ödemek durumunda kalabilir. Bu tip yazılımlardan korunmak için her şeyden önce dikkatli olmak gereklidir. E-Posta yolu ile gelmiş ve "sitemizdeki mp3leri bilgisayarınıza yüklemek için bu programı çalıştırın" veya "şifreli sayfalara erişebilmek için bu programı çalıştırın" şeklinde bir yazı gördüğünüzde

bunun numara çevirici olduğu kesindir. Kullanıcılar hiçbir şekilde bu yazılımları çalıştırmamalıdır. Bazı anticasus yazılımlar numara çeviricilere karşı da koruma sağlamaktadır. Ayrıca çevirmeli bağlantı ile internete erişilen telefon hattının milletler arası telefon görüşmelerine kapatılması da çözüm yöntemi olarak düşünülebilir.

2.2.5 Dosya türü yanıltma

Windows işletim sisteminde klasör seçeneklerindeki "Bilinen dosya türleri için uzantıları gizle" seçeneği zararlı bazı kodların gizlenmesine yardımcı olduğu için olası bir tehlikedir. Örneğin spam e-posta yolu ile gelmiş ve ekinde "resim.jpg.vbs" şeklindeki zararlı bir script kodu bilinen dosya türleri için uzantılar gizlendiğinden "resim.jpg" şeklinde bir resim dosyası olarak gözükecektir.

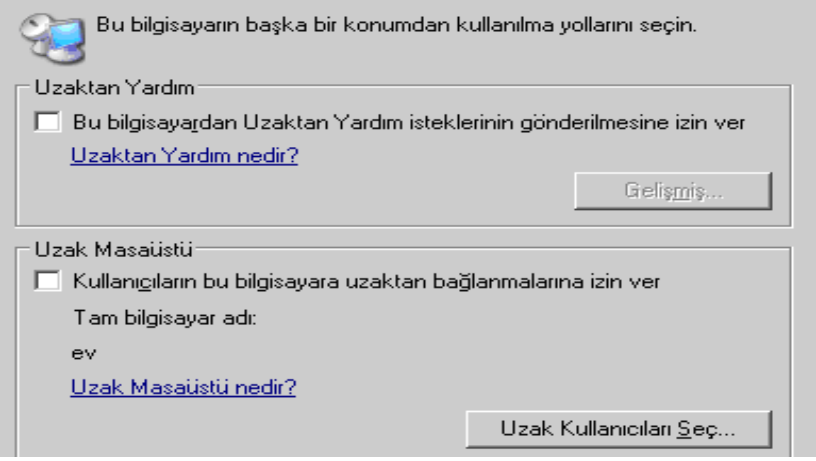


Şekil 2.2.5 Bilinen dosya uzantılarını gizle seçeneğini devre dışı bırakmak

Kullanıcı resim dosyasını açtığını zannederek bu dosyayı çalıştıracak fakat bu sırada zararlı olan script kodu çalışacak ve sistemimize zarar verecektir. Bilinen dosya türleri için uzantıları gizle seçeneğini devre dışı bırakmak için Windows gezgininde klasör seçeneklerinden bu devre dışı bırakılmalıdır (Şekil–2.2.5).

2.2.6 Erişimde Şifreleme

En yaygın tehlikelerden biride kablosuz ADSL modemlerdir. Özellile kablosuz modemlerde eğer şifreleme uygulanmazsa modemin etki alanı içindeki yabancı bir kablosuz ağ özelliği olan bilgisayar ağımıza erişebilmekte, internet bağlantımızı kullanabilmekte ve hatta özel verilerimize erişebilme ve kendine e-posta gönderebilmektedir. Bu nedenle kablosuz modemlerde şifreleme işlemi kullanılmalıdır.



Şekil 2.2.6 Uzaktan yardım ve uzak masaüstünü devre dışı bırakmak

Uzaktan erişimin de eğer kullanılmıyorsa kapalı tutulması sisteminin daha güvenli olmasını sağlayacaktır. Bunun için yapılması gereken *Denetim Masası => Sistem => Uzak* yolunu izlemek ve uzaktan erişim özelliklerini devre dışı bırakmaktır (Şekil–2.2.6).

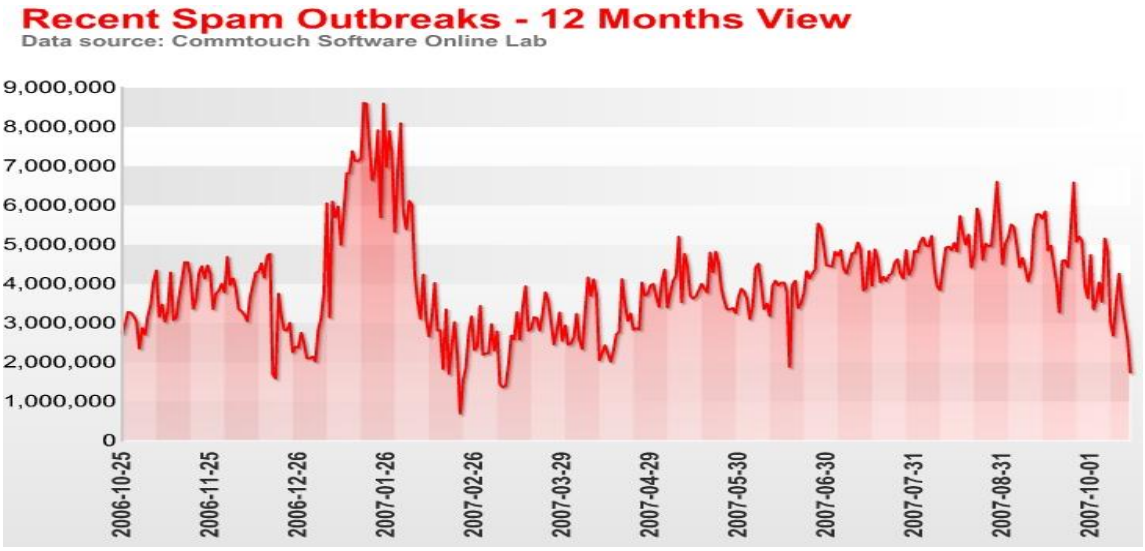
2.3 Spam Saldırılarında Karşılaşılan Beş Hata

İnternet korsanları "kurbağa tekniği" kullanırlar. E-Posta üzerinden Spam oluşturma ve bu kanaldan sızma en yaygın metoddur. Önce bir sisteme sızar, daha sonra bu sistem üzerinden diğer sistemlere sıçrarlar: Tıpkı bir kurbağanın, durgun suda bir yapraktan diğerine sıçraması gibi. Siber atakların çok büyük bir bölümü konfigürasyon hatalarından kaynaklanmaktadır. Spam saldırılarıda hataları yakından takip ederek sürekli sistemleri denemektedirler. Oysa yarını görerek bugünden önlem almak şarttır.

Oldukça büyük şirketlerden önemli bilgilerin çalındığı haberlerini artık ülkemizde de sıkça duyulur oldu. Unutmayalım ki bu siber saldırıların sebebi iyi tasarlanmamış sistemlerdir. Global terör ile ilgili havaalanındaki şu söz internet içinde aynen geçerlidir.

"Biz işimizi her zaman iyi yapmak zorundayız. Teröristlerin ise sadece bir defa işlerini iyi yapmaları amaçlarına ulaşmaları için yeterli" [15]

Şekil 2.3'de görüldüğü gibi yurt dışında özellikle hediyeleşmenin yoğun yaşandığı yıl başına yakın günlerde reklam spam saldırıları en yüksek değere ulaşmıştır.[16]



Şekil 2.3 Commtouch Software laboratuarı spam değerleri

2.3.1 Smtp Protokol Hataları

Özellikle spam saldırılarına yönelik e-posta hizmeti veren sunucu üzerindeki her protokol iyice incelemeli doğru ve gerekli tanımlamalar yapılmalıdır. Hatalı yapılandırmada en çok karşılaşılan durum smtp sunucularında karşılaşılmaktadır.

SMTP sunucu üzerine gelen postaları güvenlik duvarından NAT yaparak direk lokal ağımıza iletmek doğru değildir. DMZ adı verilen bölge güvenilir iletişim sağlamak için dizayn edilmiş bir yapıdır. Gelen postaları karşılayan sunucumuz bu bölgede bulunmalıdır.

Ayrıca DMZ bölgesine postayı karşılamak için Active Directory bilgisi taşıyan ya da Windows Domain üyesi olan bir sunucu kurulmamalıdır. DMZ ile lokal ağ arasında daha kolay iletişim sağlamak amacıyla güvenlik duvarı tanımlarında full erişim verilmemelidir.

Yapılması gereken, lokal domain veya Active Directory ile hiçbir bağı olmayan, bir e-posta sunucusu kullanmak ve bu sunucuyu DMZ bölgesinde bulundurmak. Ancak bu sayede e-posta sunucumuz bir internet korsanı tarafından ele geçirilse bile diğer sunucularımıza kolayca geçiş yapamayacaktır.

Daha güvenli bir yapının kurulması için donanım ürünleri yada açık kaynak kodlu yazılımlar kullanılarak tasarlanmış güvenlik çözümleri kullanmaktır. Bununla smtp sistemi ile lokal sistemimiz arasında bir tampon bölge hem de gelen postalar üzerinde anti-spam, virus, trojan, spyware, phishing taramasına yapılır.

Sadece antispam taraması yaparak ardı arkası kesilmeyen spam postalarla mücadele etmek zaman ve güç kaybına neden olur. Bu tip postaları sistemimiz kabul etmeden geri dönmeli(rejection code) ve spam listelerinden kendi alan adımız çıkartılmalıdır. Smtp sunucularına gelecek doğrulama(authentication) isteklerini de güvenlik politikalarına uygun olarak tanımlanmalıdır. Eğer bir güvenlik politikamız yoksa derhal hazırlanmalıdır. Sistemsel bilgilerin internetten kolayca alınmasını engellemek için varsayılan sistem etiketlerimizi değiştirmeliyiz.

2.3.2 Web-mail/POP3 Hataları

Kullanıcılar kurum veya özel elektronik postalarına erişmeleri için web-mail ve pop3 hizmetini kullanmaktadır. Kullanıcı bilgisayarlarına pop3 tanımlaması yaparak nerde olursa olsun postalarını almaları sağlanabilir. Ancak bu durumda pop3 sunucunun internetten erişebilir hale getirmesi gerekmektedir. Pop3 doğası gereği kullanıcı adı ve şifre denetimi yaptığından zayıf bir noktadır.

İkinci uzaktan posta erişim hizmeti Web-mail. En bilineni de Outlook Web Access. Ancak durum OWA'da da farklı değil. Kullanıcı adı ve şifre denetimi yapan her sistem zayıf noktadır. Ayrıca unutmamamız gerekir ki OWA sunucusu Active Directory sistemine entegredir. Yani OWA hack edilirse tüm sisteme sızılabilir.

Güvenli erşim olarak SSL-VPN kimlik doğrulama sistemi, Windows Domain sistemimizden bağımsızdır. Güvenlik çok yüksek seviyede tasarlanmıştır. Ancak buna rağmen hack edilse bile direk olarak lokal sunucularımıza sızıntı yapılamaz. Ayrıca tüm erişim SSL şifrelemesi ile sağlanır. Yani clear-text olarak çalışan smtp ve pop3 gibi sistemlerimize kolayca şifreleme sağlayabiliriz. SSL-VPN sistemlerinin yönetimi ve bakımı da çok kolaydır. SSL-VPN ürünleri ile merkez ofisimize erişimi kolaylaştıran ve güvenli kılan yatırımı yapabilir, üzerine de güvenli dosya erişimi veya full vpn hizmetlerini sağlamış olabiliriz.

2.3.3 Web Sunucuları Hataları

Hemen hemen her şirkette artık web hizmetleri var. Artık yazılımların bir çoğu web uyumlu olarak geliştiriliyor. Bu durum da internet korsanlarına yarıyor.

Açıkça söylemeliyim ki web hizmetlerinin güvenliğini sağlamak oldukça zordur. Kullanılan protokolleri çok iyi tanımak ve yazılım altyapılarını iyi bilmek gerekir. Ancak yine de web sunucumuzun http authentication yöntemlerine kolayca müdahale edebiliriz.

Web sistemimize yapılacak bir atak tüm sistemimizi internet korsanının önüne açıkça koyabilir. Sistemimizi iyi yapılandırmalıyız. SSL-VPN bu noktada yine iyi bir çözüm. Personelimizin kullandığı web uygulamalarına veya B2B sistemi kullanan iş ortaklarımıza SSL-VPN üzerinden hizmet sağlayabiliriz. Bu sayede sayıları az olan sistem kullanıcılarının erişeceği noktalarını internete bağlı herkese açmak gibi ölümcül bir hata yapmamış oluruz.

Eğer herkese açık bir sunucu varsa Reverse-Proxy veya Application Firewall ürünlerini kullanmakta fayda vardır. Söz konusu yatırımlar ve sistemlerin değeri bu yatırıma olanak tanıyacak kadar büyük olmayabilir. Ancak teknik olarak bahsedilen güvenlik sistemlerini kullanmak zorunludur.

2.3.4 Ftp Protokolü Hataları

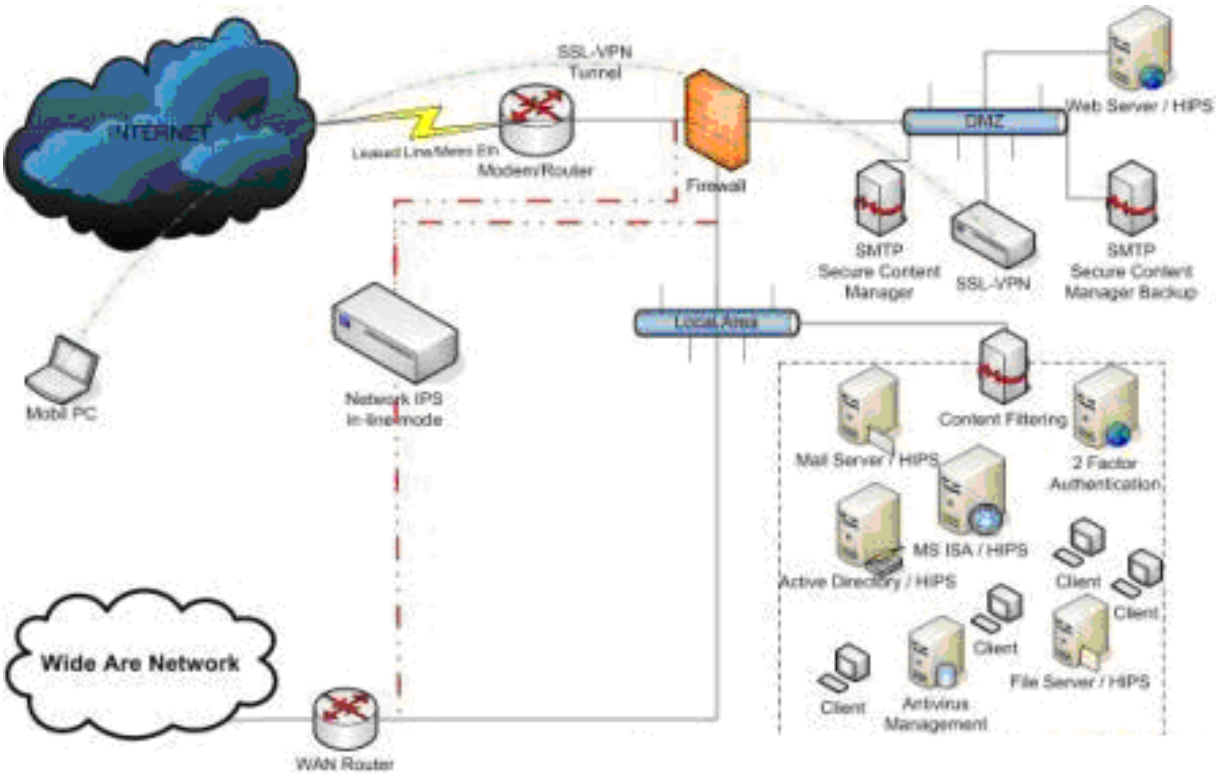
Ftp sistemi kolay dosya transferi için yaygın kullanılan protokoldür. Ancak ftp sistemini Windows Domain'i ile entegre etmek güvenlik açığıdır. Kullanacağımız ftp sunucusunun kendine ait bir authentication metoduna sahip olmasına ve mümkünse ftp sunucusunun işletim sisteminin Windows Domain'ine üye olmamasına dikkat etmeliyiz. Eğer sadece kendi personelimize veya iş ortaklarımıza hizmet veren bir FTP sunucumuz var ise yine SSL-VPN hizmeti tercih edilmelidir.

Ftp sunucusuna gerekli erişim kuralları uygulayarak sunucu üzerine başka bilgiler saklanılmamalıdır.

2.3.5 Atak Denetim Hataları

Ağ tabanlı atak engelleme sistemleri oldukça yaygınlaşmakla birlikte birçok konfigürasyon hatası yapılmaktadır.

Bu hatalardan en önemlisi konumlandırma hataları. Şekil 2.3.5'de gibi bir ağ tapısı içerisinde kullanılan güvenlik ürünlerinin çoğu birden fazla fiziksel segment üzerinde hizmet verebilir. Ağ üzerinde trafiği karşıladığı nokta mutlaka güvenlik duvarının önü olmalıdır. Bu sayede güvenlik duvarına gelecek uygulama tabanlı atakları ve DDoS ataklarını engelleyebiliriz. İkinci nokta olarak güvenlik duvarımız ile lokal ağımız arasında konumlandırılmalıdır. Ancak bu sayede lokal ağdan çıkması muhtemel atakların kaynağı tespit edilebilir. Aksi takdirde Dinamik NAT yüzünden güvenlik duvarı önünde bulunan lokal ağ kaynaklı atakların kaynak adresini güvenlik duvarının NAT adresi olarak tanımlayacaktır.



Şekil 2.3.5 Yapısal ağ üzerinde atak denetimi

Korumamız gereken diğer önemli bir nokta da şube veya b2b bağlantılarımızın lokal ağ ile buluştuğu noktadır. Bu sayede şubelerden ya da b2b bağlantılarımızdan gelecek olan atak ve solucan gibi tehditleri merkez sistemimize ulaşmadan durdurabiliriz. Aynı durumun tersi de elbette geçerli.[15]

2.4 Saldırı Çeşitleri

Buldukları en kolay yol ile güvenliğinizi bozmak isteyen saldırganlar, bunu çeşitli yöntemlerle gerçekleştirebilir. Burada neyin saldırı olarak tanımlandığının çok fazla önemi var. Bu noktada saldırıların genel bir gruplandırmasını yapmak mümkün:

2.4.1 Yetkisiz Erişim

Bu saldırı türünde, saldırgan bilgiye (yazılım, donanım ve veri) yetkisi olmadığı halde erişebilmesidir. Aynı bilgiye yetkili kullanıcılar da olağan şekilde erişebilirler, yani bilginin kendisinde bir bozulma yoktur. Bununla birlikte o bilgiye erişmesi beklenmeyen kişilerin bunu yapabilmesi, saldırı olarak nitelendirilir (örn: ağ koklama)

2.4.2 Erişim Engelleme veya Zarar Verme

Bu saldırı türünde, bilgiye erişim engellenir. Bilgi kaybolmuştur/silinmiştir, kaybolmamıştır/ulaşılamaz durumdadır veya kaybolmamıştır/ulaşılabilir durumdadır, ama yetkili kullanıcılar tarafından kullanılamaz durumdadır (örn: donanımın kırılması, veya DoS veya DDoS gibi erişim reddi saldırıları).

2.4.3 Değişiklik Yapma

Bu saldırı türü, bilginin yetkili kullanıcıya ulaşmadan önce saldırganın amaçları doğrultusunda bilgide değişiklik yapmasını içerir. Program kodları, durgun veri, veya aktarılmakta olan veri üzerinde yapılması mümkündür (örn: virüsler ve truva atları).

2.4.4 Kopyalama

Bu saldırı türü, gerçekte olmaması gereken verinin çoğaltılmasına sebep olur. Üretilen veri, daha önceki gerçek bir verinin taklidi olabileceği gibi, gerçeğe uygun tamamen yeni bir veri şeklinde olabilir (örn: sahte veri, ya da veri taklidi).

Bunların yanısıra saldırıları aktif ve pasif olmak üzere de gruplandırmak mümkün. İzinsiz erişim türündeki saldırılar pasif grupta, diğer saldırılar aktif saldırı grubunda yer alır.

2.5 İnternetteki Dolandırıcılık Yöntemleri

Gelişen teknoloji ve artan kullanıcı sayısı elektronik hırsızlığın en büyük destek noktaları, geleneksel mafyanın interneti keşfi internet bankacılığı döneminde başlamıştır. Bilgisayar ağlarına sızma konusundaki uzmanlara para yada tehdit karşılığında iş yaptıran bu grupların kimi korsanları kaçırıp silah zoruyla çalıştırmışlardır. Ancak kullanıcı sayısının ve kullanım alanının artması kullananların güvenlik konusunda en basit önlemleri bile alma konusundaki ihmallikle birleşince tam bir günlik açığı olur. Bilişim ağları üstündeki yolsuzluk ve sanal soygunlardan yıllık zararın 10 milyar doları geçtiği iddia ediliyor [17]. Elektronik ağlar üstünde en çok kullanılan suç yöntemlerinden bazıları şu şekildedir.

2.5.1 E-posta Dolandırıcılığı

Nijerya'da, Endonezya'da ya da Kenya'da darbe olmuştur ve hükümet değişmiş, askerler olaya el koymuştur. Memleketin önde gelen ailelerinden birisinin İsviçre'de yüz milyonlarca doları vardır ve bunu aktaracak bir yurtdışı hesabına ihtiyacı vardır. Hayatın garip bir cilvesi olacak; yüz milyonlarca doları olan bu adamın yurtdışında bir tane arkadaşı yoktur ve sizin hesabınıza muhtaçtır. Bu e-postaya kanarak kendi hesap bilgisini

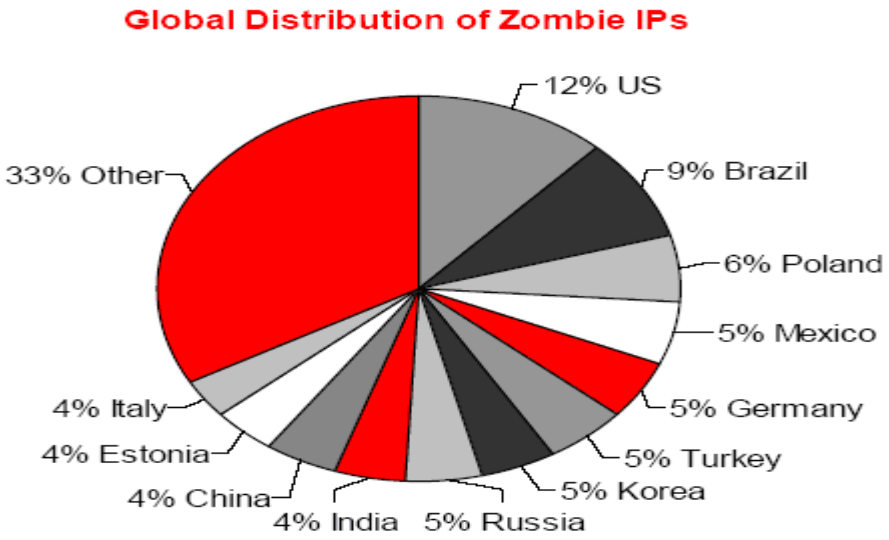
karşı tarafa verip bu paranın yarısını komisyon olarak bekleyen binlerce kişi her sene boşalan hesaplarının ardından gözyaşı döküyor. Nijerya dolandırıcılığı olarak adlandırılan bu yöntem internetteki en eski metotlardan birine örnektir.

2.5.2 Oltacılık

Bir gün bankanızdan bir e-mektup gelir. Merkez Bankası yeni sisteme geçti, bankalar çipli kart kullanmaya başlayacak gibi birbirinden enteresan gerekçelerle sizden aşağıda yer alan linke tıklayıp bankanın sitesine gitmenizi söyler. Adres bankanızın adresi gibi görünür ama tıkladığınızda açılan sayfa aynen bankanıza benzese de adresi farklıdır. Kullanıcı adınızı ve şifrenizi girersiniz, ertesi gün de boşalan hesabınızın derdine düşersiniz. Bu nedenle bankanızın sitesine girmek için her zaman adresi elimizle yazmamız gerekir.

2.5.3 Zehirlenmiş bilgisayarlar

Bilgisayarınızda durduk yere reklam pencereleri açılıyor, antivirüs yazılımınız (varsa) çalışmaz hale geliyor, sisteminiz her gün biraz daha yavaşlıyorsa zararlı yazılımlardan biri bulaşmıştır. Bu tip kontrolü başkasına geçmiş bilgisayarlara 'zombi' deniyor.



Şekil 2.5.3 Commtouch GlobalView Reputation service

Yukarıdaki şekilde görüldüğü gibi elinde on binlerce bu tip bilgisayar bulunan zombi zenginleri reklam, spam yollamak ya da ticaret sitelerine saldırıp fidye istemek için kullanmaktadırlar. Anti-virüs, Anti-trojan, Anti-spyware, Anti- casus, Anti-Spam yazılımlarını bilgisayara kurmayı ihmal etmemek gerekmektedir. [16]

2.5.4 Kablosuz ağ avcılığı

Taşınabilir bilgisayarlar kablosuz ağlara bağlanma yeteneği kazanınca herkese açık internet erişim noktaları mıknatıs gibi kullanıcıları çekmeye başladı. Hatta kimi cafeler müşteri çekmek için bunu bir araç olarak kullanmaya başladı. Ancak bu tip ağlarda(WiFi) etrafınızda dizinin üstünde bilgisayarıyla oturan yetenekli birinin yazdığınız her şeyi (şifreleriniz de dâhil) öğrenmesi veya bilgisayarınıza casus yazılımlar yüklemesi son derece kolay ve elde edilebilir bir ortamdır. Bu nedenle şifreli ssl bağlantısı olmayan yerlerden erişim oldukça tehlikelidir.

2.5.5 İlgi istismarı

Popüler olaylar sırasında milyonlarca kişinin bilgi edinmek için internet sitelerine yöneldiğini bilen gruplar bu merakı sömürmek için fırsatı kaçırmıyor. Örneğin en son Dünya Kupası sırasında katılımcı takımların adına ekran koruyucu dağıtan bir kaynağın aslında bilgisayarlara virüs yüklediği ortaya çıkmıştı. Aynı şekilde Saddam Hüseyin'in idam videosunu yüklemeye çalışırken bilgisayarına en zararlı casus yazılımların bilgisayara kurulduğu ve ele geçirildiği gözlemlenmiştir.

BOLUM–3

3 AĞ ORTAMINDA DOLAŞAN ZARARLI YAZILIMLAR

3. 1 Zararlı Yazılım

Genel olarak tüm zararlı yazılımlar; yaşam döngüsü, kendi kendini çoğaltma, özerklik, bulaşma mekanizması, ayrık veya virüs özelliği taşıma, korunma mekanizması açısından farklı karakteristikler sergileyebilmektedir. Zararlı yazılımlar, yaşam döngüsünde her hangi bir aşamada farklı davranışlar sergileyebilecekleri gibi, kendi kendini çoğaltmayacak tek bir amaca yönelik çalışmakla birlikte kullanıcının araya girmesine ihtiyaç duyabilecekleri gibi tamamen özerk bir yaklaşıma sahip olabilmektedirler.

Spam kaynaklı zararlı yazılımlar, gelişme süreçleri açısından belirgin karakteristik özellikleriyle bilgi ve bilgisayar güvenliğine karşı önemli tehditler içeren ve oldukça yaygın bir şekilde kullanıcıların maruz kaldığı yazılımlardır. Virüs, solucan, Truva atı ve mesaj sağanağı (spam) gibi kullanıcıların nispeten farkında olduğu türler dışında var olan diğer ana türler takip eden kısımda incelenmiştir.

3.1.1 Zararlı Yazılımdaki Amaç

Zararlı yazılımlar ne kendiliğinden var olabilirler ne de yazılımlardaki hatalardan (bug) türeyebilirler. Programcılar ya da virüs oluşturma yazılımı kullanan kişiler tarafından üretilirler. Bilgisayar virüsleri ancak programlandığı etkinlikleri gerçekleştirmeye muktedirdir. Bunların zararlıyı üretme ve yayma amacı çok çeşitli nedenlere dayandırılabilir. Bu tür yazılımlar araştırma projeleri amaçlı, şaka amaçlı, belirli şirketlerin ürünlerine saldırmak amaçlı, politik mesajları yaymak amaçlı ve ya kimlik hırsızlığı, ajan yazılım ve saklı virüs ile haraç kesme gibi yöntemlerle finansal kazanç sağlamak amaçlı yazılabilmektedir. Bazı virüs yazıcılar ürettiklerini sanat yapıtı olarak görmekte ve virüs yazmayı bir tür hobi olarak tanımlamaktalar. Ek olarak birçok virüs yazıcısı, virüslerin sistemler üzerinde tahrip edici etkiler göstermesinden yana değildir. Bulaştıkları programları güvenlik açısından geliştirilmeye zorlar ya da diğer virüsleri silerler. Bu tür virüsler çok nadirdir ve sistem kaynaklarını kullanır, bulaştıkları sistemlere yanlışlıkla zarar verebilir ve bazen diğer zararlı kodların bulaşması ile virüs taşıyıcı hale gelebilirler. Zayıf yazılmış bir yazılım dahi yanlışlıkla zarar veren forma dönüşebilir. Birçok hukuk sahasında herhangi bir bilgisayar zararlısını yazmak suç sayılmaktadır.

3.1.2 Gelişim Süreci

Zararlı yazılım (malware, İngilizce "malicious software'in kısaltılmışı), bulaştığı bir bilgisayar sisteminde veya ağ üzerindeki diğer makinelerde zarara yol açmak veya çalışmalarını aksatmak amacıyla hazırlanmış istenmeyen yazılımların genel adıdır. Zararlı yazılımlar, kullanıcının haberi olmadan veya kullanıcıyı yanıltarak sistemlere yetkisiz bir şekilde bulaşmaktadır.

Kirli yazılım (scumware) olarak da ifade edilen zararlı yazılımlar, hemen hemen her programlama veya betik (script) dili ile yazılabilmekte ya da birçok dosya içinde taşınabilmektedirler. [18]

Tarihi gelişim açısından Zararlı yazılımlar, dört kuşakta incelenebilir :

I. Kuşak (1987–1995): Bilgisayar virüslerinin özellikle DOS virüslerinin egemen olduğu bu kuşakta Zararlı yazılımlar, dosya ve disketler aracılığıyla bulaşmaktaydı. 1995 yılında korunmuş kipte ilk işletim sistemi olan Windows 95 işletim sistemi ile dönemlerini tamamlamışlardır.

II. Kuşak (1995–2000): Kişisel bilgisayar dünyasında yaşanan gelişmeler ışığında özellikle resim, ses ve video gibi materyaller içeren çoklu ortam desteği içeren dosyaları kullanan Microsoft Word, Excel gibi ofis programları ile beraber gelen ve güçlü yeteneklere sahip makro dilini kullanan zararlı yazılımların yoğunlukta olduğu bir kuşaktır. Win32 platformuna yönelik makine diline yeterince hâkim olamayan kişiler için makro dili bulunmaz bir imkân sunmuştur. Makrolar hâlâ kullanılsa da, virüs tarama programlarının yaygınlaşması ile bu dönem sona ermiştir.

III. Kuşak (1999–2004): Özellikle İnternet kullanımı ve e-posta iletişimin artması ile kitle postacılarının (mass mailler) arttığı bir dönemi kapsayan bu kuşakta, özellikle e-posta ve İnternet tarayıcı programlarında yer alan açıklardan istifade edilmektedir. Bu dönemde zararlı yazılımlar, çeşitli betik dillerinin sunduğu imkânlardan istifade etmekte ya da e-postalara eklenen dosyaların içinde sistemlere bulaşma yolunu seçmiştir. E-posta filtreleme programları ile bu tür zararlı yazılımlarının engellemesi ile belirli bir doyuma ulaşılmıştır.

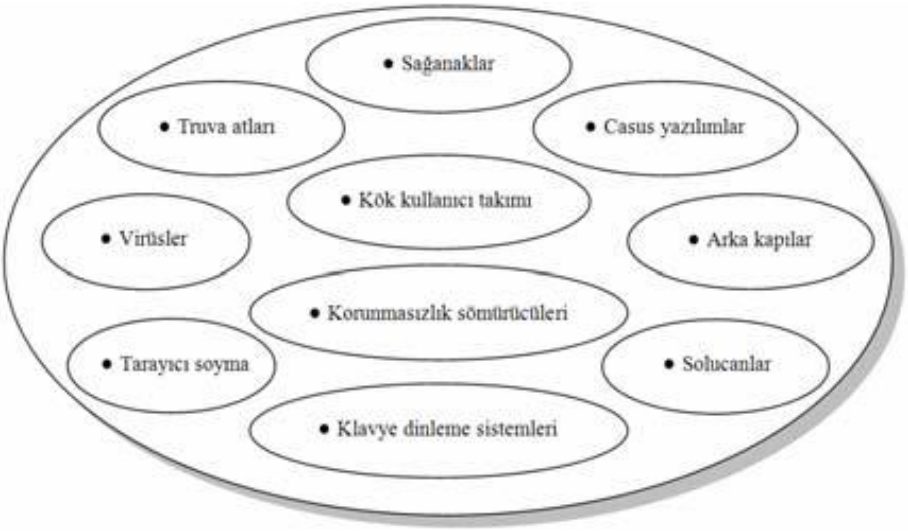
IV. Kuşak (2004– …): Halen devam eden bu kuşağın diğer kuşaklardan en önemli farkı, yayılmak için belirgin bir kullanıcı yardımına ihtiyaç duymamasıdır. Zararlı yazılımlar sistem ve programlarda bulunan korunmasızlıklardan yararlanmaktadır. Bu dönem ile özellikle yasadışı ve suç içeren sonuçlar doğuracak ve ciddi zarar veren zararlı yazılımlar

yaygınlaşmaya başlamıştır. Bu kuşak ile beraber, klavye dinleme sistemleri gibi kendi kendini çoğaltmayan zararlı yazılımlar da ortaya çıkmıştır.

Şekil 3.1.2'de şema şeklinde gösterilen virüsler, solucanlar (worm), Truva atları (Trojan horse), arka kapılar (backdoor), mesaj sağanakları(spam), kök kullanıcı takımları gibi özellikle internet üzerinden yayılan zararlı ataklardır.

Bu yazılımlar; (Main types of Malware), (rootkit), telefon çeviriciler (dialer), korunmasızlık sömürücüleri (exploit), klavye dinleme sistemleri (keylogger), tarayıcı soyma (browser hijacking) ve Ajan yazılımlar (spyware) en genel zararlı yazılımlardır.

Zararlı yazılımların etkileri konusunda son yıllarda yapılan inceleme çalışmaları, konunun ciddiyetini gözler önüne sermektedir.



Şekil 3.1.2 Zararlı yazılımın ana türleri

• "Code Red" solucanı İnternet üzerindeki korunmasız bilgisayarların hepsine 8 saatte bulaşabildi. Slammer solucanı aynı işi 20 dakikada yaptı. Bir IM korunmasızlık sömürüsü yarım milyon bilgisayara 30 saniye içinde yayıldı(Symantec Security Response).

• 2001 yılında her 300 e-postada bir virüs bulunurken; 2004 yılında bu sayı her 100 e-postada bir virüse düştü (MessageLabs).

• 1993–2003 yıllarında gerçekleşen saldırı sayısı on kat artarak 1344 rapor edilmiş saldırıdan 137529 saldırıya çıktı (CERT Coordination Center). Günlük rapor edilen yeni veya değiştirilmiş virüs tehdidi 20 ile 40 arasına artmıştır(Reuters).

• Geniş bant bağlantısı olan bilgisayarların yaklaşık %90'nında Ajan yazılım bulunduğu tahmin edilmektedir (Scott Culp, Microsoft).

• Ajan yazılımlar bütün Windows uygulama çökmelerinin üçte birinden sorumludur (Scott Culp, Microsoft).

• 2003 yılında virüslerin iş dünyasına maliyeti yaklaşık 55 milyar ABD $'dır (TrendMicro).

• 3 milyon işyeri bilgisayarının ele alındığı bir araştırmada 83 milyon Ajan yazılım saptandı (Gartner Group, Eylül 2004).

• Siber saldırılardan kaynaklanan kayıpların 2004'ün bitimi ile 16,7 milyar $'a çıkması beklenmektedir. 1997 yılında bu nedenle ortaya çıkan kayıplar 3,3 milyar $'dı (Computer Economics, 2004).

• Şirketlerin %96'sı virüs korunma yazılımları kullanmalarına rağmen; bu şirketlerin zarar gördükleri saldırıların %78'i yine virüs ve solucanlardır (2005 CSI/FBI Computer Crime and Security Survey).

• Forrester'ın hazırlamış olduğu raporda, bilişim teknolojilerinde karar vericilerinin %40'ının, Zararlı ve Ajan yazılımlar hakkında bilgilerinin olmadığı ve Ajan yazılımlardan etkilenip etkilenmediklerini bilmedikleri ortaya çıkmıştır (Forrester, 2005 [8]).

• Symantec, 2004 yılının ikinci yarısında 7360'dan fazla yeni Zararlı yazılım tespit etmiştir. Bu sayının, 2004 yılı ikinci yarısından %64 oranında daha fazla olduğu açıklanmıştır (Symantec Internet Security Threat Report, 2005).

3.2 Zararlı Yazılımın Etkileri

Bazı virüsler uygulamalara zarar vermek, dosyaları silmek ve sabit diski yeniden formatlamak gibi çeşitli şekillerde bilgisayara zarar vermek amacıyla programlanmışlardır. Bazıları zarar vermektense, sadece sistem içinde çoğalmayı ve metin, resim ya da video mesajları göstererek fark edilmeyi tercih ederler. Bu zararsızmış gibi gözüken virusler kulanıcı için problem yaratabilir. Bilgisayar hafızasını işgal ederek makineyi yavaşlatabilir, sistemin kararsız davranmasına hatta çökmesine neden olabilirler. Ek olarak birçok virüs, hata (bug) kaynağıdır ve bu hatalar sistem çökmelerine ve veri kaybına neden olabilir.

Bilgisayar ağlarının yaygınlaşmasından evvel, birçok virus çıkarılabilir ortamlar ,özellikle disketler, vasıtasıyla yayılmaktaydılar. Geleneksel bilgisayar virüsleri de 1980'lerde kişisel bilgisayarların hızla yayılması başlangıç oldu günümüzde ise ağ dosya paylaşımları ve e-postalarla çığ gibi büyümüştür. Virüs bulaştığı makineyi kullanarak bir web adresi linkini kişiler listesindeki tüm şahıslara hazır mesaj olarak gönderebilir. Mesajı alan kişi arkadaşından (ya da herhangi bir güvenilir kaynaktan) geldiğini düşündüğü linke tıklarsa, ulaşılan sitede bulunan virüs bilgisayara bulaşabilir ve yukarıda bahsedilen yöntemi kullanarak diğer kurban bilgisayarlara yayılabilmektedir. Bu nedenle yazılım ve donanım tedbirleri zorunlu hale gelmiştir.

Alınan Toplam Veri Miktarı	125.969Mb
Alınan Toplam İleti Sayısı	2.410.931
Geri Çevrilen İleti Sayısı	108.230
Bounce Eden İleti Sayısı	179.646
Drop Edilen İleti Sayısı	1.199.668
Kullanıcıya İletilen İleti Sayısı	923.387

Tablo 3.2 TÜBİTAK'ın 2004 - 2005 yılında aldığı virus içeren e-posta miktarı

Tablo 3.2'deki örnek çalışmada da görüldüğü gibi dünya çapındaki istatistikler de göz önünde bulundurulduğunda, e-posta iletişimini sağlayan altyapının çok büyük bir kısmı SPAM e-postaların taşınması için çalışmaktadır.

3.2.1 Sosyal Deformasyon ve Etkilenme

Kullanıcıların bilgisayar ve İnternet kullanımı esnasında karşılaşabilecekleri sosyal deformasyonlar genel olarak aşağıdaki şekilde gruplanabilir:

- Teknik zararlar; çocukların bilgisayara virüs bulaştırması, casus yazılımların girmesine müsaade etmesi, bilgisayarın bozması. Program ve dosyaların kaybedilmesi ve bazı yazılım ayarlarının bozulması sonucu oluşan olumsuz ruh hali.
- Fiziksel, sosyal ve psikolojik zararlar; aşırı oyun oynamak, dışarıda ya da okulda arkadaşlarıyla etkileşimde olmak yerine eve kapanmak ve şiddet içerikli oyunlar oynamak gibi bilgisayar ve İnternet kullanımının neden olabileceği zararlar.
- Hayati zararlar; zararlı içeriklere erişim, kötü niyetli kişilerle teması ve istismarı.
- İnternet ortamında bilinçsiz kullanıcılar; beklenilmeyen ve istenilmeyen tehditlerle, tehlikelerle ve durumlarla karşı karşıya kalabilirler. Bunlar;

- Pornografik öğe, düşmanlık, öfke ve şiddet ihtiva eden yasa dışı içeriğe İnternet üzerinde maruz kalabilme,
- Çevrimiçi ortamlarda, kendilerini veya ailelerini tehlikeye atacak adres, kredi kartı numarası, evde o an kimin ya da kaç kişinin bulun-duğu bilgisi gibi bilgileri üçüncü şahıslara, eposta veya sohbet programları vasıtasıyla iletebilme,
- İnternet üzerinden ebeveynlerinin kredi kartı ile haber vermeden alışveriş yapabilme,
- Kendisinden yaşça büyük ve kötü niyetli kişi-lerle ve suç örgütleri ile haberleşebilme gibi konular olabileceği gibi; daha farklı ve tehlikedeki şekillerde de kendini gösterebilir. Bütün bu riskler, konunun önemini gözler önüne sermeye yeterlidir.

İngiltere'de 2006 yılında yapılan bir araştırmaya göre; Çevrimiçi pornografiye rastlamak % 57, başka bir şey yaparken pornografik çıkıveren reklâm görmek% 38, Başka bir şey ararken bir porno sitesine kazara girmek % 36, pornografik mesaj sağanağı almak % 25, Şiddet ve korku içeren bir siteye rastlamak % 22, düşmanca ve nefret dolu bir siteye rastlamak % 9 olarak tespit edilmiştir.[19]

Görüldüğü gibi kullanıcılara yönelik tehdit ve riskler son derece ciddidir. İnternet kullanıcılarını bilgisayar ve İnternet'in nimetlerinden doğru, etkin ve verimli bir şekilde yararlanması sağlanırken, güvenlikleri her zaman ön planda tutulmalıdır. Ayrıca İnternet üzerinde istenmeyen e-posta içeriklerine karşılaşmakta diğer bir önemli tehdit, kötü niyetli kişilerleirin ticari rantı haline gelmiştir. İnternette sohbet ortamında tanışmalar dolayısıyla dolandırıcılık ve cinayetlere kurban gitmek internetin bir başka sorun boyutunu oluşturmaktadır.

3.3 Bilgisayar Virüsleri

Kullanıcının izni ya da bilgisi dahilinde olmadan bilgisayarın çalışma şeklini değiştiren ve kendini diğer programların dosyaları içerisinde gizlemeye çalışan aslında bir tür bilgisayar programıdır.

Bilgisayar virüs programları önemli dosyaları silmek veya konak (host) sistemini tamamen çalışmaz hale getirmek gibi yıkıcı etkileri bulunmaktadır. Bu virüsler, bilgisayar solucanının bir parçası olarak ağ üzerinden yayılabilir olmalarına rağmen yayılmak için ağ kaynaklarını kullanmazlar. Bunun yerine disket, CD veya DVD gibi ortamlarla veya e-posta eklentileri ile hedef sistemlere bulaşırlar. Bir dosyanın açılmasıyla, bir e-postanın

okunmasıyla, bir sistemi önyüklemesiyle (boot) veya virüs bulaşmış bir programı çalıştırması ile kullanıcı farkına varmadan virüsü yayar.

3.3.1 Dosya virüsleri

Dosya virüsleri yürütülebilir dosyalara tuttunan ve konak program çalıştırıldığında etkinleşen kod parçaçıklarıdır. Etkinleştikten sonra, virüs kendini diğer program dosyalarına tutturarak yayılabilir ve programlandığı şekilde kötü niyetli faaliyet gösterebilir. Kendilerini sistem hafızasına yükleyip sürücüdeki diğer programlar çalıştığında etkinleştirecek şekilde değiştirir. Yayılmalarının yanı sıra bir tetikleyici vasıtasıyla etkinleşen tahrip edici bir tür bileşeni bünyelerinde barındırırlar. Tetikleyici özel bir tarih , virüsün belirli bir kopyalama sayısına ulaşması ya da önemsiz herhangi bir şey olabilir. Randex, Meve and MrKlunky dosya virüslerine verilebilecek birkaç örnektir.[20]

3.3.2 Önyükleme virüsleri

Bir önyükleme sektörü virüsü, sabit diskin çok önemli bir bölümü olan önyükleme sektörünü (boot sector) etkiler. Önyükleme sektörü sabit diske ait tüm bilgilerin saklandığı ve bir program vasıtası ile işletim sisteminin başlatılmasını sağlayan yerdir. Virüs , her açılışta hafızaya yüklenmeyi garantilemek amacıyla kodlarını önyükleme sektörüne yerleştirir. Bu disketle daha çok yayılıyordu CD-ROM döneminin başlamasıyla kendni doğrudan CD ye kaydedemez hale gelmiştir. Önyükleme virüsleri hala var olsa da işletim sistemlerinin artık önyükleme sektörlerini özel koruma altına almışlardır. Polyboot.B ve AntiEXE önyükleme virüslerine örnektirler.

3.3.3 Çok parçalı virüsler

Çok parçalı virüsler önyükleme sektörü ve dosya virüslerinin birleşimidir. Bu virüsler CD/DVD, disket, e-posta gibi enfekte olmuş ortamlar ile gelir ve hafızaya yerleşirler. Akabinde sabit diskin önyükleme sektörüne taşınırlar. Sektörden de sabit diskteki yürütülebilir dosyalara (.exe) bulaşır ve tüm sistem boyunca yayılırlar. Çok parçalı virüsler kolay temizlenebildiğinden pek yayılamamaktadır. En bilineni Ywinz'dir.

3.3.4 Makro virüsler

Makrolar içeren çeşitli program ya da uygulamalarca oluşturulmuş dosyalara bulaşan virüslerdir. Word, excel, powerPoint, access, corel draw gibi uygulamalarla oluşturulmuş dosyalarla yayılmaktadır. Makro virüsler işletim sisteminin değil ait olduğu uygulamanın

dilinde yazıldığından platform bağımsızdırlar ve uygulamayı çalıştırabilen tüm işletim sistemleri (Windows, Mac vb.) arasında da yayılabilirler. Uygulamalardaki makro dillerinin süreki artan kabiliyetleri ve ağlar üzerinde yayılma olasılıkları bu türden virüsleri büyük tehdit haline getirmektedir. Relax, Melissa.A ve Bablas makro virüs örnekleridir.

3.3.5 Ağ Virüsleri

Ağ virüsleri, yerel ağlarda ve hatta İnternet üzerinde hızla genelde paylaşılan kaynaklar, paylaşılan sürücüler ya da klasörler üzerinden yayılırlar. Ağ üzerindeki potansiyel hedefleri araştırarak saldırıya açık savunmasız sistemleri bulduklarında ağ virüsü sisteme bulaşır ve benzer şekilde tüm ağa yayılmaya çalışırlar. Nimda ve SQLSlammer kötü nam salmış ağ virüslerindendir.[19]

3.3.6 E-posta virüsleri

Bir eposta virüsü, kendini konağın eposta adres defterindeki bağlantılara gönderen bir makro virüs şeklinde olabilir. Eğer herhangi bir eposta alıcısı özellikle spam şeklinde gelen viruslü emaildeki ekleri açar ise , virüs eposta adres defterine bulaşır ve kendini listedeki kişilere gönderir. Gününüzde eposta virüsleri, mail istemci (Outlook, Thunderbird) üzerinden eposta önizlemesi yapıldığında dahi sisteme bulaşabilecek durumdadırlar.

3.3.7 Eşlik virüsleri

Eşlik virüsleri dosyalara tutunarak değil EXE, COM ve EXD uzantılı yeni dosyalar oluşturur.. Eğer kullanıcı belirli bir programı çalıştırmak için komut konsoluna sadece programın ismini yazıp .EXE uzantısını yazmayı unutursa DOS işletim sistemi aynı isimli COM uzantılı dosyada öncelik olduğundan ajan dosyayı çalıştırabilir.

3.3.8 Yazılım Bombaları

Yazılım bombaları, gerekli şartlar oluşana dek atıl durumda kalan ve özel bir kodu işleyen yazılımlardır. Şartların olgunlaşması kullanıcıya mesajlar göstermek ya da dosyaları silmek gibi belirli fonksiyonları tetikleyecektir. Yazılım bombaları bağımsız programların içerisinde barınabildikleri gibi virüs ya da solucanların parçaları da olabilirler. Saatli bomba benzeri daha önceden zehirlenen bilgisayarlar belirlenen tarih geldiğinde otomatik olarak çalışırlar. Ünlü Friday the 13th virüsü buna örnek verilebilir.

3.3.9 Cross-site scripting virüsleri

Bir cross-site scripting virüsü (XSSV) çoğalabilmek için cross-site betik açıklarını kullanan virüslerdir. Kendisini otomtik çalışan script yazılımlar şeklinde web uygulamaları ve web tarayıcıları üzerinde çalışan virüs tipi yazılımlardır.

3.3.10 Sentineller

Oldukça gelişkin virüs tipi olup bulaştığı bilgisayarları uzaktan kullanma yetkisi verir. Sentineller köle adı verilen elde ettiği bilgisayarlarda hizmet engelleme saldırısı gibi kötü niyetli amaçlarda kullanılacak geniş ağlar oluşturmada kullanılırlar.

3.3.11 Yerleşik olmayan virüsler

Yerleşik olmayan virüslerin keşfedici modül ile çoğaltıcı modülden oluştukları düşünülebilir. Keşfedici modül virüsün bulaşması için kullanılacak yeni dosyalar aramakla yükümlüdür. Keşfedici modülün karşılaştığı her yürütülebilir dosyaya çoğaltıcı modül çağrılmak suretiyle virüs bulaştırılır.

3.3.12 Yerleşik virüsler

Yerleşik virüsler çoğaltıcı modülü içerir keşfedici modül bulunmamaktadır. Virüs yürütüldüğü vakit çoğaltıcı modül hafızaya yüklenir ve böylece işletim sistemi belirli tip bir görevi her seferinde uygularken çoğaltıcı modülün de yürütülmesi sağlanır. Örneğin işletim sistemi bir dosyayı her seferinde yürütürken çoğaltıcı modül çağrılabilir. Bu durumda virüs bilgisayarda yürütülmekte olan tüm uygun programlara bulaşabilir.

3.4. Bilgisayar Solucanları

Bilgisayar virüslerine benzer bir yapıda olup virüsler gibi bir başka çalıştırılabilir programa kendisini iliştirmez veya bu programın parçası olmazlar. Solucanlar, yayılmak için başka bir programa veya insan etkileşimine ihtiyaç duymaz, kendi kendini çoğalır. En yaygın yöntemler arasında, e-posta, FTP ve HTTP gibi İnternet hizmetleri bulunmaktadır. Solucanlar, başka dosyaları değiştirmezler; fakat etkin bir şekilde bellekte dururlar ve kendilerini kopyalarlar. Solucanların kontrol dışı çoğalmaları, sistem kaynaklarını aşırı kullandığında veya diğer işlemekte olan görevleri yavaşlattığında bu görevlerin sonlanmalarına neden olduğunda farkına varılabilir.

Bilgisayar solucanları; e-posta, IM (Internet Messaging), İnternet ve ağ solucanları olmak üzere dört grupta incelenebilir. Daha çok spamle yayılan e-posta solucanları, zararlı yazılımların en çok tercih ettikleri yayılma yöntemi olan e-postaları kullanmaktadır.

Genellikle bir fotoğraf veya metin dosyası gibi tek bir eklenti içerecek şekilde gönderilen e-postaların içerisinde bulunurlar. Kullanıcı eklentiyi çalıştırdığında solucan kendini başlatır ve konak makineye bulaşır. Solucanlar genellikle bulaştıkları makinede kullanıcının adres defterinden e-posta adreslerini toplar ve kendini bulduğu her bir adrese gönderir(spam).

"İnternet Mesajlaşma" (IM) Microsoft'un MSN Messenger, AOL'nın AIM, IRC, ICQ, KaZaA gibi yaygın mesajlaşma hizmetleri ve ağ paylaşımları IM solucanlarının yayılması için kullanılırlar. Hedeflenen hizmeti kullanan tüm kullanıcılara, solucan bulaşmış bir dosya veya solucanın kendisinin yer aldığı bir web sitesine yönelen İnternet bağlantısı gönderirler [5]. Bağlantıya tıklandığında solucan bilgisayara indirilir ve otomatik olarak çalışır. Solucan kendini konak makineye kurar ve kullanıcının haberleşme listesindeki tüm kullanıcılara aynı türde spam mesajlar göndererek kendini yaymaya devam eder.

İnternet solucanları, ağ ve İnternet üzerinde tarama yapar en son güvenlik güncellemelerini kurmamış olan, açık kapıları olan veya güvenlik duvarı olmayan korunmasız bilgisayarları bulur ve kendini kurar. W32/Blaster ve W32/Deloder bu tür solucanlara örnektir.

Bir başka türü ağ solucanları, paylaşılan bir klasöre, isimlerini faydalı veya ilginç gözükebilecek bir uygulama veya dosya ismine dönüştürerek kendilerini kopyalarlar. Bu dosyaları çalıştıran kullanıcılar kendi bilgisayarlarına solucanı bulaştırmış olur.

3.5 Truva Atları

Truva atları ilgi çekici görünen ama aslında aldatmaya yönelik zararlı dosyalardır. Sistemde var olan dosyalara kod eklemektense ekran koruyucu yüklemek, emaillerde resim göstermek gibi bir işle iştigal oldukları izlenimi uyandırırlar. Ancak , aslında arka planda dosya silmek gibi zararlı etkinlikler gerçekleştirmektedirler. Truva atları bilgisayar korsanlarının bilgisayarınızdaki kişisel ve gizli bilgilerinize ulaşmalarına imkan tanıyan gizli kapılar da yaratırlar.

Truva atları virüs gibi kendilerini çoğaltamazlar. Yayılması için saklı bulunduğu email eklentisinin açılması ya da Truva atını içerir dosyanın internet üzerinden bilgisayara indirilip yürütülmesi gerekir. Bir Truva atı faydalıbir programa "bohçalanabileceği" (bundling) gibi; kullanıcıları, faydalı bir işleve sahip olduğunu ikna edip, bizzat kullanıcı tarafından çalıştırılmaları ile de etkinleştirilirler. Sisteme çeşitli şekillerde zarar veren

genel Truva atları dışında, PSW Truva atları, Truva arka kapıları, tıklayıcılar, indiriciler, damlalıklar, vekiller, Ajanları, bildiriciler ve arşiv bombaları aşağıdaki türlerde Truva atları bulunmaktadır.

3.5.1 Truva arka kapıları ve PSW

En yaygın ve tehlikeli Truva atı türüdür. Bulaştığı makinenin uzaktan kontrolünü sistem yöneticisinin farkına varmadan saldırgana veren araçlar içerir. PSW ise kişisel bilgisayarda bulunan şifreleri çalmak için kullanılan Truva atlarıdır.

3.5.2 Truva tıklayıcılar

İnternet tarayıcıların ayarlarını değiştirerek veya İnternet adresleri ile ilgili işletim sistemi dosyalarını değiştirerek hedef kullanıcının belirli bir siteye veya İnternet kaynağına yö-neltmeyi sağlayan Truva atıdır. Bu tür Truva atları, bir İnternet sitesinin ziyaretçi sayısını artırarak, reklâm veren firmaların dikkatini çekmek ve İnternet arama motorlarının siteyi daha popüler olarak listelemesini sağlamak için veya ileride yapılacak olan bir saldırı için hedef bilgisayarın kullanılmasını sağlamak amacıyla kullanılmaktadırlar. Truva tıklayıcılar DoS (Hizmet Aksattırma, Denial of Service) saldırıları için kullanılmaktadır.

3.5.3 Truva indiriciler

Bu tür Truva atları, hedef makineye yeni bir zararlı yazılım veya reklâm yazılımı indirip ve kurmak için bir ara basamak oluşturur. İndirici, kullanıcının haberi olmadan yeni Zararlı yazılımı indirip çalıştırır veya sistem açıldığında otomatik olarak başlatır. İndirilecek Zararlı yazılımın adresi Truva atı içinde bulunmaktadır.

3.5.4 Truva damlalıkları

Truva indiricileri gibi damlalıklar da başka bir Zararlı yazılımın sisteme yerleşmesini sağlayan bir ara basamak vazifesi görür. Bu tür Truva atları içinde muziplik içeren bir dosyayısadece sisteme yüklediğini hissettirerek programın sebep olduğu etkinliğin zararsız olduğunu düşündürür. Hâlbuki bu Truva atının asıl amacını yerine getiren diğer yükler için bir maskedir.

3.5.5 Truva vekilleri

Bu Truva atları, hedef makinenin İnternet erişimini bir vekil sunucu (Proxy server) gibi saldırganın hizmetine açar. Mesaj sağanağıoluşturmak isteyen kötü niyetli kişiler, bu tür yoğun mesajlaşma için hedef bilgisayarın kaynaklarını kullanmaktadır.

3.5.6 Truva Ajanları

Tuş basımları, ekran görüntüleri, etkin uygulama kayıtları ve diğer kullanıcıfaaliyetlerini toplayan ve bu bilgileri saldırgana gönderen Truva atlarıdır.

3.5.7 Truva bildiriciler

Saldırgana Truva atının bulaştığını bildiren yapılardır. Hedef bilgisayara ait IP adresi, açık kapı numaraları ve e-posta adresleri gibi bilgiler e-posta, ICQ v.s. ile veya saldırganın web sitesine gönderilir.

3.5.8 Arşiv bombaları

Bu tür Truva atları, sıkıştırılmış arşiv dosyalarını açan programları sabote etmek için kodlanmış arşiv dosyalarıdır. Çalıştırıldığında, hedef bilgisayar yavaşlar ve çöker veya disk ilgisiz verilerle doldurulur. Gelen verilerin otomatik olarak işlendiği sunucular için bu tür Truva atları çok tehlikeli olabilir. Arşiv dosyasında hatalı başlık bilgisi oluşturarak; arşiv içindeki verileri tekrar ederek ve aynı dosyaların arşivlenmesi ile bu tür Truva atları oluşturulmaktadır. Tekrar eden verilerden oluşan büyük bir dosya çok küçük bir arşiv dosyası olarak paketlenebilir. Örneğin 5 GB bir veri RAR biçiminde 200 KB kadar sıkıştırılabilir.

3.5.9 Hizmeti engelleme Truva atları

Hizmeti engelleme saldırısı (Denial of service attacks) Truva atlarının dayandığı temel düşünce kurbanın bilgisayarındaki İnternet trafiğini bir web sitesine ulaşmasını veya dosya indirmesini engelleyecek şekilde arttırmaktır. Hizmeti Engelleme Saldırısı Truva atlarının bir başka versiyonu mailbombası(spam)dir. Ana amaçları mümkün olabildiğince çok makineye bulaşmak ve belirli email adreslerine aynı anda filtrelenmeleri münkün olmayan çeşitli nesneler ve içerikler ile saldırmaktır.

3.5.10 Vekil sunucu Truva atları

Bu türden Truva atları bulaştığı bilgisayarı vekil sunuculara çevirir. Saldırgan o bilgisayarı kullanarak alan adı kaydı(DNS) yönlendirmesi yapabilir. Belli sitelere çalıntı kredi kartları ile erişebilir ve kanunsuz birçok işi iz bırakmadan kendini gizleyerek gerçekleştirebilir.

3.5.11 FTP Truva Atları

Bu tür Truva atları en basit ve artık modası geçmiş Truva atlarıdır. Yaptıkları tek şey FTP transferleri için kullanılan 21. portu açmak ve herkesin bilgisayarınıza bağlanabilmesine

imkan tanımaktır. Bu türün yeni versiyonları sadece saldırganın sisteminize ulaşmasını sağlayan parola korumalı yapıdadırlar.

3.6 Ajan Yazılımlar (Spyware)

Bilgi ve bilgisayar güvenliğinde ajan yazılım, genelde muğlâk bir anlamda kullanılmaktadır. Ajan yazılım, kullanıcılara ait önemli bilgilerin ve kullanıcının yaptığı işlemlerin, kullanıcının bilgisi olmadan toplanmasını ve bu bilgilerin kötü niyetli kişilere gönderilmesini sağlayan yazılım olarak tanımlanır. Ajan yazılımlar, diğer zararlı yazılımlara göre özellikle İnternet kullanıcıları tarafından sistemlere farkında olmadan bulaştırılmaktadırlar. Ajan yazılımlar, virüs ve solucanlardan farklı olarak hedef sisteme bir kez bulaştıktan sonra kendi kopyasını oluşturarak daha fazla yayılmaya ihtiyaç duymazlar. Ajan yazılımın amacı kurban olarak seçilen sistem üzerinde gizli kalarak istenen bilgileri toplamaktır. Bu bilgi kimi zaman bir kredi kartı numarası gibi önemli bir bilgi bile olabilir . Bunun dışında, ticari firmalar İnternet üzerindeki kullanıcı alışkanlıklarını saptamak amacıyla ajan yazılımları İnternet üzerinde yayabilmektedirler . Kullanıcıların haberi olmadan sistemlere bulaşabilen ajan yazılımlar, kişisel gizliliğe karşı gerçekleştirilen en önemli saldırılardan biridir [21].

Sistemlere bulaşmaması için bilgisayar sisteminin, yama ve güncellemelerle sürekli güncel tutulması ve İnternet üzerinde bilinmeyen programların indirilip, çalıştırılmaması gibi önlemler ajan yazılımlara karşı da korunma sağlayacaktır. Bunun dışında nasıl virüslere karşı virüs korunma yazılımları kullanılıyorsa; son zamanlarda gelişme gösteren karşı Ajan yazılım (anti-spyware) ürünleri de bilgisayarların vazgeçilmez araçları olarak anti-virüsler gibi sistemlere kurulup en güncel halleri ile kullanılmalıdır.

3.7 Arka Kapılar (Backdoor)

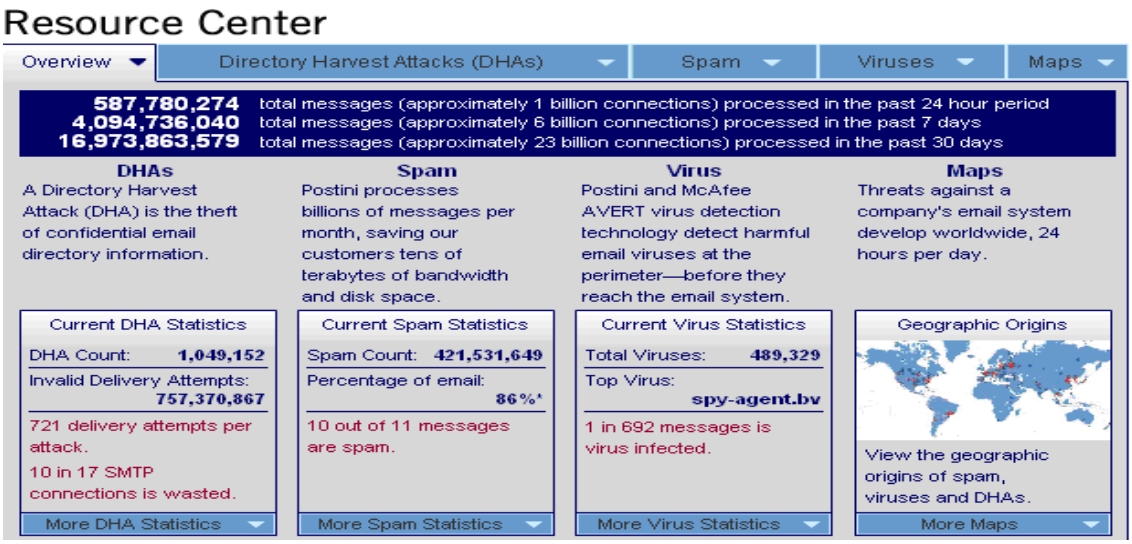
Bilgisayar üzerinde sıradan incelemelerle bulunamayacak şekilde, normal kimlik kanıtlama süreçlerini atlamayı veya kurulan bu yapıdan haberdar olan kişiye o bilgisayara uzaktan erişmeyi sağlayan yöntemler, arka kapı olarak adlandırılmaktadır. Bir sisteme sızmak için oldukça zahmetli bir çaba harcayan korsanlar, daha sonra aynı sisteme erişmek için daha kolay bir yolu sisteme eklemek isterler. En sık karşılaşılan arka kapı yöntemi, hedef sistemde, dinleme ajanı iliştirilmiş bir kapıyı (port) açık tutmaktır. Bu açıdan bakıldığında, bu tür bir açığa maruz kalındığından emin olmak için, sistemde mevcut bulunan bütün kapılar, 1'den 65535'e kadar, iki kere (bir kez TCP bir kez de UDP için) taranmalıdır [20].

Arka kapılar, çoğunlukla Truva atları ile karıştırılabilmektedirler. Her ikisi de hedef sisteme sızmaya yaraya Zararlı yazılımlardan; Truva atı, faydalı bir program gibi gözükürken; arka kapı, sadece sisteme erişimi sağlayan gizli yapılardır.

Arka kapılar kimi zaman, sistemi geliştiren programcı tarafından test edilen sisteme erişmek amacıyla kullanılan fakat daha sonra unutulan açıklar olabilmektedir. Bu durumun bir şekilde farkına varan kötü niyetli kişiler, bu yapıları kullanabilirler. Hatta bu tip arka kapılar bazen programcı tarafından kasten bırakılabilmektedir [21].

3.8 Mesaj Sağanakları(Spam)

Mesaj sağanakları (spam, junkmail), belki de kullanıcıların günlük hayatta en sık karşılaştıkları ve sıkıntı çektikleri zararlı yazılımların başında gelmektedir. Sağanak, reklâm, ürün tanıtım ve satma veya diğer kötü amaçlarla kişilerin e-posta hesaplarına istemedikleri mesajlarla meşgul etmesidir. IDC'e göre 2003 yılında dünya çapında gönderilen e-posta sayısı 7,3 milyardır. Ferris Research'ün yapmış olduğu araştırmaya göre sağanaklar 4 milyar $'lık bir verimlilik kaybına yol açmaktadır [23]. Symantec'in Mayıs 2005 sağanak raporuna göre, dünya çapında sağanak olarak tanımlanan mesajlar, bütün mesajların %60'ıdır. Yine aynı araştırmaya göre sağanak mesajların %82'si İngilizce mesajlardır.



Şekil 3.8 Ekim-2007'de commtouch güvenlik firması spam tespit değerleri

Sağanakların sebep olduğu bu zararlardan korunmak için bu tür e-postaları süzen yazılımlar e-posta programları ile tümleşik olarak çalışmaktadır. Bunun dışında bu tür mesajların sonunda yer alan ve mesaj listesinden çıkmak isteyen kişiler için sunulan

listeden çıkma bağlantılarına şüphe ile yaklaşmak gerekir. Bu bağlantılar bilinen ve güvenilir kaynaklar haricinde, sağanağı gönderen kişi veya gruba e-posta hesabının kullanılan gerçek bir hesap olduğunu göstermektedir. Rasgele hesap adları üretip sağanak gönderen kişiler, gerçek bir kişiye ait olduklarını saptadıkları bu e-posta adreslerini üçüncü kişilere pazarlayarak daha fazla sağanağa neden olmaktadırlar.

3.8.1 Reklâm

Reklâm yazılımın zararlı yazılım olması şart değildir, fakat bu tür yazılımlar, bir bedava veya paylaşımlı yazılımdan (freeware veya shareware) beklenebilecek reklâm anlayışının ötesinde yöntemler kullanırlar. Daha çok reklâmlar, programlama maliyetini karşılamaya; kullanıcılara daha düşük fiyat sunmaya ve programcılara yeni uygulamalar geliştirmesi ve yaptıkları uygulamaları idame etme ve güncellemesi için cesaret vermeye yönelik yararlı yönleri bulunmaktadır. Bu tür programlar reklamlarını, çıkıveren pencerelerde (pop-up window) veya ekranda bir şeritte (banner, reklâm bandı) yer alacak şekilde yapmaktadır.

3.8.2 Parazit Yazılım

Parazit yazılım, üyelik (affiliate) yöntemi ile başka firmaların ürünlerinin satılmasına aracılık ederek gelir elde eden sitelerdeki iz sürme bağlantılarını silen reklâm yazılımı türüdür. Bu davranış, üyelikle elde edilecek komisyon veya kredilerini etkilediğinden, "parazit" olarak nitelendirilmektedir. Kullanıcı için önemli bir güvenlik tehdidi değildir.

3.8.3 İz Sürme

İz sürme çerezlerinin üstüne yazarak veya İnternet tarayıcılarında o anki trafiği, yeni tarayıcı pencereleri açarak farklı sitelere de yönlendiren ve bu şekilde üyelik komisyonlarını çalan uygulamalardır. Bunun yanında bu tür yazılımlar, kullanıcının ziyaret etmekte olduğu sayfalara kendi bağlantılarını da ekleyebilmektedir [11].

3.8.4 İstenilmeyen Yazılım

Reklâm yazılım türünde olup çoğunlukla ikiyüzlü üreticiler tarafından, kullanışlı bir program olarak sunulan yazılımlardır. Sisteme büyük zararlar vermeyen bu tür programlar, bilgisayar kullanımı sırasında verdikleri rahatsızlıklarla, diğer sıradan programlarda olduğu gibi otomatik olarak bilgisayardan kaldıracak bir yöntemin kasten sunulmamasıdır.

Bu yazılımlar müşteri çekmek amacıyla, sistemde yer işgal eden işe yaramayan artık dosyaları kolayca veya otomatik olarak temizleme, sistemin güvenliğini artırma, sistemin bilgi işleme gücünün etkinliğini geliştirme, eğlenceli oyunlar, çok özellikli İnternet

tarayıcı, daha ilginç fare işaretçi imgeleri ve ekran koruyucularıve daha iyi arama motoru sunma vaadinde bulunmaktadırlar [1]. Bu yazılımlar CPU, bellek ve bant genişliği gibi sistem kaynaklarını hoyratça kullandığı veya kullanım sırasında anormal sıkıntılarla günlük çalışma verimliliğini olumsuz yönde etkilemektedir.

3.8.5 Tarayıcı Yardımcı Nesnesi

İnternet Gezgini (Internet Explorer) her açıldığında otomatik olarak çalışan, genel olarak tarayıcıya diğer yazılımlar tarafından yerleştirilir ve tipik olarak araç çubuğu donatıları tarafından kurulur. Zararlı amaçlı olup, İnternet tarayıcısına kurularak kullanıcıya ait İnternet'te erişilen her bilgiyi toplayabilir ve kullanım verilerini gizlice izleyebilir.

3.8.6. Uzaktan Yönetim Aracı

Saldırgana çevrim içi olduğunda bu makineye sınırsız erişim hakkı veren en tehlikeli zararlı yazılımlardan biridir. Saldırgan, bu araçları kullanarak dosya aktarımı, dosya ve programların eklenme ve silme işlemleri, fare ve klavyeyi kontrol altına alma, kullanıcıya yanıltıcı çeşitli sistem veya uygulama mesajları gönderme gibi işlemleri kolaylıkla yapabilir. Uzaktan yönetim araçları, özellikle şirketlerden bilgi kaçırmak için oldukça sık kullanılan yaklaşımlardandır.

3.8.7. Bilgisayarı Ele Geçirme

Uzaktan yönetim yazılım türü olan, kötü niyetli kişiler tarafından mesaj sağanağı (spam) göndermek, izinsiz daha fazla Ajan yazılım kurmak gibi kötü amaçlara yönelik kontrol altına aldıkları, bilgisayar solucanları ve Truva atları gibi zararlı yazılımların çalıştırıldığı, ele geçirilmiş bilgisayarlardan oluşmaktadır.

Birçok arama motorunun İnternet üzerindeki sayfaları ortaya çıkarmak amacıyla kullandığı ve web sayfalarını inceleyip sayfanın içerdiği bağlantılara yönelip diğer sayfaları tarayan örümcekler (spider) ve tırtıllar (crawler), en yaygınları arasındadır.

3.8.8. Ağ Taşkını

DoS hizmet aksattırma saldırılarına sebep olacak şekilde, seri PING (Packet Internet Groper, Paket İnternet Yoklayıcı) veya SYN (eş zamanlama) paketi göndermek gibi yöntemlerle, bir ağ bağlantısına veya makineye kasten aşırı yük bindiren yazılımlar, sırası ile ölümüne PING (Ping of Death) ve SYN ağ taşkını olarak adlandırılmaktadır [19]. Bunun dışında sistem günlüğüne (log) defalarca aynı kayıtların tekrarlanması ile günlüğün

büyüklüğünü artırarak sistemlere zarar vermeye çalışan mesaj taşkınısaldırıları da bulunmaktadır.

3.8.9. Saldırgan ActiveX

Genellikle kullanıcıların bilgisayarlarına kaçak indirme ile (drive-by-download), İnternet Gezginine kurulan yazılımlardır. Bu tür bir uygulama, sisteme bir kez kurulunca, bilgisayar üzerinde normal bir program gibi, genelde kullanıcıdan gizli olarak çalışabilir ya da diğer Zararlı yazılımları indirip, kurabilir. Bazı saldırgan ActiveX yazılımları meşru ve imzalı ActiveX kontrollerinin adını kullanarak da, kötü niyetlerini saklayabilmektedirler [11].

3.8.10. Saldırgan Java

İnternet tarayıcıları, Java programını sarmalayan (encapsulate) ve yerel makineye erişimi önleyen bir sanal makineye (virtual machine) sahiptir. Bir Java uygulamacığının (applet) arkasında yatmakta olan teori, çalıştırılan uygulamacığın, büsbütün bir uygulama olmasından ziyade; tıpkı ekran üzerinde gösterilen yazı ve şekiller gibi bir içerik sunacak şekilde çalışmasıdır. Bu şekilde Java yazılımlarının sistem güvenliğini tehdit etmediği düşünülmekteydi. 2000 yılında, bilinen bütün tarayıcıların aslında, bu "kum torbalarını" (sandbox) aşacak güvenlik açıklarına sahip olduğu anlaşıldı. Birçok güvenlik uzmanı bu durum karşısında, ya Java seçeneğini etkisiz kılmayı ya da daha ileri kum torbaları ve sanal makinelerle Java uygulamalarını sarmalamayı önermektedir.

3.8.11. Saldırgan Betik

.VBS, .WSH, .JS, .HTA, .JSE ve .VBE uzantılı metin dosyalarından oluşan ve Microsoft WScript veya Microsoft Betikleme Konak Uygulaması (Microsoft Scripting Host Application) tarafından yürütülen metin dosyaları, istenmeyen faaliyetleri icra etmek amacıyla kullanılabilmektedir. Bu tür betikler, içerdikleri Zararlı niyet açısından saldırgan betik olarak adlandırılmaktadır.

3.8.12. IRC Ele Geçirme Savaşı

IRC (Internet Relay Chat), popülerliliğini yitirmemiş sohbet programlarından biridir. IRC savaşları uzun süre IRC şebekesini rahatsız etmiştir. IRC şebekesinde çalışmakta olan iki sunucu, bir birleri arasındaki bağlantıyı kaybedince, her iki tarafta, kısaca "op" olarak adlandırılan ve o kanalı idare eden kanal operatörlerinin sahip olduklarıyetki ve konumlar korunmalıdır. Eğer oluşan kopma sırasında sunucuların herhangi birinde bir kullanıcı bulunmuyorsa; kanala o sırada tekrar katılan insanlar, kanal operatörü konumunu

kazanabilirler. Sunucular daha sonra birleşince de asıl operatörler kanaldan atılabilir (kick out). Bu, daha ileri saldırılar için iyi bir zemin sağlayabilir [34]. Verilen bu örnek dışında, IRC üzerinden yapılan her türlü saldırıyı kolaylaştırmak amacıyla kullanılan tüm araçlar, IRC savaşı olarak sınıflandırılmaktadır [5].

3.8.13. Nuker

Uygun şekilde yamalanmamış veya güvenlik duvarıolmayan Windows işletim sistemli makinelere yapılan WinNuke DoS saldırısı için kullanılan "nuke" terimi (nuke: nükleer silah), şu an için çeşitli TCP/IP DoS saldırılarının genel adı olarak da kullanılmaktadır[22]. Ticari yazılımların yasal olmayan biçimde dağıtıldığı"warez" adı verilen bilgisayar dünyasında "Nuker", warez grubunun kurallara uymasını denetleyen kişilere verilen addır.

3.8.14. Paketleyici

Bir prosesin içine bir dosyayışifreleyerek sıkıştıran yardımcı programlardır. Program çalıştırıldığında, bellekteki dosyayı kendiliğinden açan bir başlığı prosese ekler[23]. Paketleyiciler, Truva atı geliştiricileri tarafından, çalışmalarının virüs korunma ürünleri tarafından saptanmasınıönlemek için kullanılmaktadır.

3.8.15. Ciltçi

Dosya yönetimi açısından ciltçi, Microsoft'un ciltçi yazılımı gibi, türleri farklı da olabilecek birden fazla dosyayıtek bir dosya haline getiren yazılımlardır. Fakat ne yazık ki bu tip dosyaların içine Truva atlarıgibi Zararlı yazılımların da paketlenmesi mümkündür. Bu yüzden Microsoft dâhil birçok yazılım üreticisi, bu tip yazılımları üretmeyi bırakmışlardır.

3.8.16. Şifre Yakalayıcılar ve Şifre Soyguncular

Sistemde girilen şifreleri yakalayıp kaydetmeye yönelik çalışan Ajan programlardır. Bu tür programlar konak içinde çalışabileceği gibi ağ üzerindeki paketler içinde hesap ve şifre bilgilerini saptayıp, elde edebilmektedirler [18].

3.8.17. Şifre Kırıcılar

Kaba kuvvet ve sözlük tabanlı deneme yanılma yöntemlerini de içeren; bir şifreyi veya şifreli bir dosyanın şifresini çözen araçlardır. Şifre kırıcılar, güvenlik yöneticileri tarafından meşru bir biçimde, kullanıcılar tarafından tanımlanmış olan zayıf şifrelerin bulunması ve bu şifrelerin değiştirilmesinin, daha güvenilir bir sistem oluşturmak için, kullanıcıdan talep edilmesi için de kullanılabilmektedir.

3.8.18. Anahtar Üreticiler

Yazılımların yasal olmayan yollarla kopyalanmasınıönleyerek, lisanslıyazılım kullanıma sevk etmek amacıyla oluşturulan anahtar (yazılım lisans numarası) tabanlı yazılım korumalarını, meşru anahtarlar üreterek kıran araçlardır. Bu araçları kullanan kişiler, yazılımısatın almadan kopyalayıp kurdukları programlardan, yetkili kullanıcı gibi faydalanabilirler.

3.8.19. E-posta Hasatçısı ve Bombalayıcı

Hedef kişinin e-posta gelen kutusunu (inbox), binlerce e-posta ile bombardıman eden zararlı yazılımlardır. Gönderilen e-postalardan, gönderen kaynağın bilgisini elde etmek mümkün değildir. Mesaj sağanağı oluşturmak veya sazan avlamak isteyen kötü niyetli kişiler için, insanların kendi kişisel bilgisayarlarında bulunan özel ve dış dünyaya yayılmamış e-posta adreslerini elde etmek çok önemlidir. Bu sayede çok sayıda gerçek kişiye erişmek mümkün olmaktadır. E-posta adres hasatçıları, çeşitli yöntemlerle bilgisa-yarlarda sabit disklerde bulunan e-posta adreslerini veya adres listelerini kullanıcıdan habersiz, bir sunucuya iletirler. Mimail virüsü bu amaçla hazırlanmış hasatçılara bir örnektir. E-posta adres hasatçılarını tespit etmek için daha önce hiç kullanılmamış bir "iz sürme" eposta adresi yem olarak kullanılabilir. Bu adrese gelen ilk e-posta iletisini gönderen kişinin, e-posta adres hasatçısı ile ilişkili olduğu iddia edilebilir. 1987'de yaşanan ilk CHRISTMA EXEC solucanı ve 1999 yaşanan Melissa virüsü, bu tür zararlı yazılımlarla yayılmıştır. [23]

3.8.20. Web Böcekleri

İz sürme böceği (tracking bug), piksel etiketi (pixel tag), web feneri (web beacon) veya temiz GIF (clear GIF) olarak da bilinen web böceği, HTML tabanlı bir e-posta mesajını veya bir web sayfasını kimlerin, kaç kez görüntülediği ve mesajla ne kadar süre ilgilendiği gibi bilgileri elde etmek amacıyla kullanılan ilginç ve sıradan kullanıcı tarafından pek bilinmeyen bir tekniktir. Web böceği, saydam veya artalan renginde ve genelde 1x1 piksel boyutunda küçük bir resimdir. Bu resim, mesajın içine gömülmediğinden, e-posta programının mesaj penceresinde gösterilebilmesi için harici bir adresten indirilmektedir. Resmin dosya olarak bulunduğu bu bağlantının hareketlerinin kaydını tutan web sunucusu, mesajı okuyan kişinin IP adresini, resmin gösterilme süresini ve buna benzer birçok bilgiyi elde edebilmektedir. Bu tür bir mesajı açan kişi, en azından kendi e-posta adresinin geçerli

ve kullanılan bir adres olduğunu karşı tarafa ifşa etmektedir. Bu şekilde ileride birçok mesaj aynı e-posta adresine gönderilebilir.

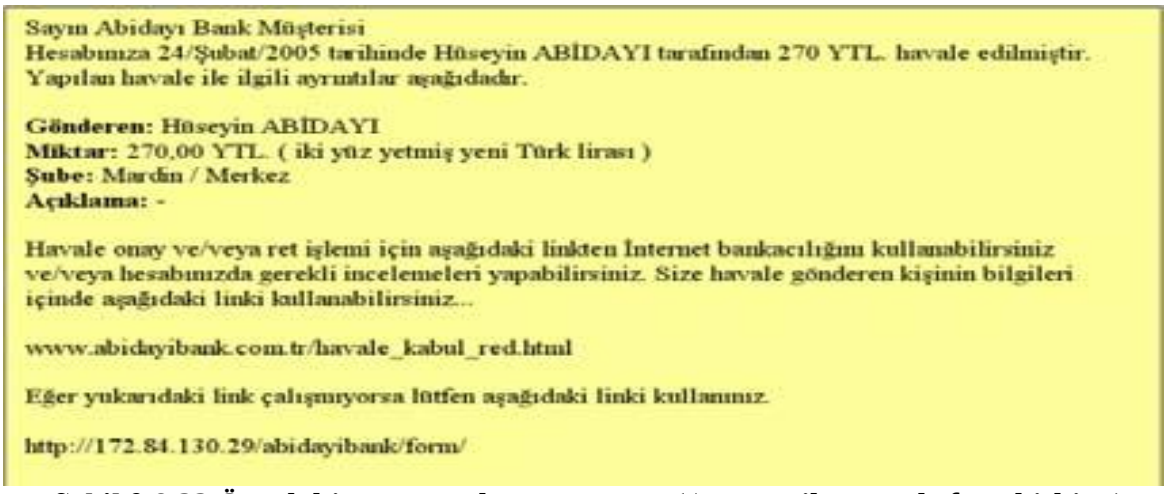
3.8.21. Aldatmaca

Kullanıcıları, olmayan bir şeyin varlığına ikna etmeyi amaçlayan her türlü "numara", aldatmaca olarak sınıflandırılmaktadır. Aldatmacanın en yaygın biçimde gerçekleşen türü, aslında olmayan bir virüs ya da Zararlı yazılım hakkında insanları uyaran mesaj sağanaklarıdır. Bunun dışında inanılması zor hayali olaylar, dini veya insani konular içeren çeşitli aldatmaca mesajları ve ünlü veya önemli kişilerden geliyormuş gibi gönderilen mesajlar, sık sık kullanıcılara iletilmektedir. Bir mesajın aldatmaca olduğunun farkına varamayan kişiler, mesajı yardımcı olmak amacıyla başka kişilere de ileterek, aldatmacanın daha da fazla yayılmasına alet olurlar. Bu tip aldatmacalar, gereksiz İnternet trafiğine ve zaman kaybına yol açmaktadır. Bunun dışında örneğin önemli bir işletim sistemi dosyasını, zararlıbir dosya gibi gösteren aldatmacaya inanan kişi, belirtilen dosyayı silerse sistemin tamamen çalışmamasına neden olabilmektedir. Bu yüzden, aldatmaca türünde mesajları hiç dikkate almamak yerinde bir davranış olacaktır.

3.8.22. Kimlik Hırsızlığı

Dilimizde kullanılmak amacıyla "sazan avlama" phishing, kimlik hırsızlığı (identity theft) adı verilen banka hesap numaraları, kredi kartınumaraları gibi kişisel bilgilerin, banka gibi resmi bir kurumdan gerçekten gönderilen resmi bir mesaj gibi gözüken e-postalarla kişilerden elde edilmesidir. Sosyal mühendisliğin bir uygulama alanı olan bu tür sahte e-postalarını alan kişi, istenilen gizli bilgileri göndererek, bu bilgilerin kötü niyetli üçüncü şahısların eline geçmesine ve akabinde oluşabilecek zararlara maruz kalınmasına neden olacaktır. Amerika'da 57 milyon insanın farklı teknikler kullanılarak sazan avlamaya maruz kaldığı ve sazan avlama sebebi ile 2003 yılında 500 milyon $'lık bir kayıp ortaya çıktığı rapor edilmiştir[23].

Şekil 3.8.22'te bir örneği gösterilen e-posta'ya benzer birçok mesaj, bugünlerde ülkemizde de insanlara gönderilmektedir. Örnek e-posta'da, varolan hiç bir bankayı ima etmemek adına burada "Abidayı" olarak isimlendirilen bir bankadan gelen mesajda, gönderilen kişinin hesabına bir para havalesinin yapıldığı "müjdeleniyor". Kurbandan bu havaleyi kabul edip etmediğini, bankanın resmi İnternet adresinden girerek doğrulaması isteniyor.


Sayın Abidayı Bank Müşterisi
Hesabınıza 24/Şubat/2005 tarihinde Hüseyin ABİDAYI tarafından 270 YTL. havale edilmiştir.
Yapılan havale ile ilgili ayrıntılar aşağıdadır.

Gönderen: Hüseyin ABİDAYI
Miktar: 270,00 YTL. (iki yüz yetmiş yeni Türk lirası)
Şube: Mardin / Merkez
Açıklama: -

Havale onay ve/veya ret işlemi için aşağıdaki linkten İnternet bankacılığını kullanabilirsiniz ve/veya hesabınızda gerekli incelemeleri yapabilirsiniz. Size havale gönderen kişinin bilgileri içinde aşağıdaki linki kullanabilirsiniz...

www.abidayibank.com.tr/havale_kabul_red.html

Eğer yukarıdaki link çalışmıyorsa lütfen aşağıdaki linki kullanınız.

http://172.84.130.29/abidayibank/form/

Şekil 3.8.22 Örnek bir sazan avlama e-postası(An e-mail example for phishing)

Bu işlem için kurbana verilen adres (www.abidayibank.com.tr/ havale_kabul_red.html) ise, gerçekte bankanın resmi internet sitesinde var olmayan bir sayfayı işaret etmektedir. Bu adres, bölge adı şeklinde değil de, IP numarası (http://172.84. 130.29) şeklinde, rakamlarla veriliyor. Bu adresi bankanın resmi bir adresi olarak algılayıp belirtilen adrese giden kişi, hesap bilgileri ve şifrelerini, korsanın daha önce hazırladığı sahte banka sayfasından, korsana bizzat kendi elleriyle verebilmektedir.

3.8.23. Web Sahtekârlığı ve Dolandırıcılığı

İnternet üzerinden veya e-posta ile yapılan bir dolandırıcılık türüdür. Kişileri maddi veya manevi zararlara uğratacak türde etkileri olan ve İnternet üzerinde yapılan girişimler web sahtekârlığıolarak adlandırılmaktadır. Nijerya yatırımı (Nigerian investment), saadet zinciri ya da piramit entrikası(pyramid schemes) ve mektup zinciri (chain letters) en sık rastlanan web sahtekârlıklarındandır. Ülkemizde de örneklerine rastlanan mektup zinciri, gönderilen kişiye maddi zarara uğratmaz; fakat bu kişi aldığı mesajı örneğin 10 kişiye göndermezse pek yakında kötü bir felakete uğrayacağı şeklinde korkutularak zincirin devamı sağlanır. Bu tür mesajlar hiçbir şekilde ciddiye alınmamalıdır. Nijerya yatırımı türünden web sahtekârlığında, mesajın gönderildiği kişiden Nijerya gibi Afrika ülkelerinde bulunan bir bankada var olduğu söylenen yüklü bir miktardaki paranın dışarıya transferine yardım edilmesi istenmektedir. Bu yardım karşılığında kendisine yüklü miktarda bir pay verileceği belirtilir. Mesajı alan kişiden kendi ülkesinden kendisinin sahip olduğu bir banka hesap numarasını, mesajı gönderen ve kendisini önemli biri veya bir hükümet görevlisi olarak tanıtan kişiye iletmesi talep edilir. Buna inanan kişi transfere aracılık etmek istediğinde işlemin tamamlanması için kendisinden işlemin yapılabilmesi için yüksek miktarda ücret talep edilir ve nihayetinde kurban binlerce dolar zarar edebilir. Saadet zinciri ise kişilerin

zincirde var olan bir kişinin altına belirli bir ücret ödeyerek üye olduğu ve üye olduktan sonra kendisine dâhil olacak üyeler getirdiği sistemlerdir. Üyelerin piramidin üstündeki kişilere ev, araba, dizüstü bilgisayar gibi mallar aldırmaya yarayan sistemler bu tür saadet zincirlerine örnektir. Bunların dışında deniz aşırı piyango veya bahis konularında, iş bulma, evden para kazanma konularında, define arama konularında, yardım ve bağış konularında ve geleceği görme gibi mistik konularda kişileri zarara uğratabilecek web sahtekârlıkları da bulunmaktadır. Kullanıcılar, çabuk zenginlik, şöhret veya başarı vadeden bu tür mesajları hiçbir şekilde ciddiye almamalıdır.

3.8.24. Port Tarayıcılar

Herhangi birinin bir port'u dinleyip dinlemediğini görmek amacı ile bir makine üzerinde tanımlı olan 65 536 adet port'un hepsini otomatik olarak sınayan araçlardır [5]. Bu araçlar, önlem almayan sistemlere sızmak veya sistemden bilgi kaçırmak için kullanılabilmektedir.

3.8.25. Güvenlik Tarayıcı

Olası korunmasızlıkları aramak amacıyla başka bir sistemi araştıran araçlardır. Sondaj araçları, güvenlik durumlarını desteklemek isteyen güvenlik yöneticileri tarafından meşru bir biçimde kullanılabileceği gibi; bir sisteme ne tür bir saldırı yapılabileceğini araştırmak isteyen saldırganlar tarafından da kötü amaçlarla kullanılabilir. Bu tür araçlara örnek olarak NT Güvenlik Tarayıcı (NT Security Scanner) verilebilir.

3.8.26. Arama Motoru Soyguncusu

İnternet tarayıcıların varsayılan arama motoru ayarlarınıdeğiştirmek amacıyla hazırlanan Zararlı yazılımlardır. Bu şekilde arama yapmak isteyen kullanıcının sorgularıveya olmayan veyahut yanlış girilen bir adres sonucu açılacak, varsayılan arama sayfası, başka bir siteye yönlendirilmektedir.

3.8.27. Koklayıcı(Sniffer)

Bir ağ üzerindeki IP paketlerini "koklamak" için kullanılan donanım ve yazılımlar, koklayıcı olarak adlandırılmaktadır. Koklayıcı yazılım veya donanım, bütün paketleri dinleyen ayrımsız kipe (promiscuous mod) geçerek bütün ağ trafiğini dinler ve kaydeder. Bu paketler içinde yer alan şifre bilgileri gibi önemli bilgiler, paket içeriği taranarak elde edilebilir. Ağ üzerinde kullanılan aktif ağ cihazları, paketleri sadece ulaşılmasıistenen adrese yönlendirerek, koklayıcıların paketleri elde etmesinin önüne geçebilmektedir. UNIX sistemlerinde ifconfig komutunun çıktısında PROMISC bayrağı bulunuyorsa sistemde koklama yapılıyor demektir.

3.8.28. Kandırıcı(Spoofer)

Kandırıcılar, saldırganın IP adreslerinin sahtelerini üretmek (IP kandırma, IP spoofing) amacıyla kullanılır. Şirinler (Smurf, çizgi film) ve Fraggle (Muppet şov'daki ad) saldırıları, bugünlerde kullanılan kandırma saldırılarının en başında gelenleridir. Saldırılmak istenen hedef makinenin adresi, paketi gönderen adres olarak yazıldığıbir sahte paketin, bir yayın (broadcast) adresine gönderilmesi ile bu saldırılar başlatılır. Yayın bölgesinde var olan bütün makineler hedef makineye cevap paketlerini gönderir. Bu da hedef makinenin İnternet bağlantısına aşırı yük bindirir. IP kandırıcıdışında, başka isimle e-posta gönderme ve sahte web sitesinin yayınlanmasıyla yapılan web kandırıcı yöntemleri de bulunmaktadır.

3.8.29. Ajan Yazılımı ve İz Sürme Çerezleri

Sitelerin İnternet üzerinde daha kullanışlı bir hizmet vermek amacıyla kullandıkları çerezler, kötü amaçlara da hizmet verebilmektedir. Kişisel kullanıcı bilgilerinin elde edilmesi ve paylaşılması amacıyla bu çerezler kullanılabilmektedir.

Bir kullanıcının İnternet üzerinde gezinme geçmişini izlemek amacıyla, iki veya daha fazla web sayfasında paylaşılan çerezler iz sürme çerezleri olarak adlandırılmaktadır.

3.8.30. İnternet Gezinme Alışkanlıkları

Birçok tarayıcı ve karşı ajan yazılımların iz sürme çerezlerini engellemeleri sonucunda ortaya çıkan arayışın son örneklerinden biridir. Bu yöntemlerin başında, Macromedia Flash MX uygulamasının yerel paylaşılan nesneleri (local shared objects) gelmektedir. Flash canlandırmaları son zamanlarda web sayfalarında oldukça yaygın bir şekilde kullanılmaktadır. Bu tür canlandırmaları oynatabilen programlar arasında Macro-media Flash Player, Mart 2005'e göre % 98 ile birinci sırada bulunmaktadır. Flash biçeminde bir reklâm içeren bir web sayfası, bir çerez gibi işlev gören SOL uzantılı bir dosyayı genellikle "\ Documents and Settings \ {kullanıcı_adı} \ Application Data \ Macromedia \ Flash Player \" klasöründe alt klasörlerin altında tutmaktadır. İşte bu dosyaların incelenmesiyle, kullanıcıların İnternet'te gezinme alışkanlıkları rahatlıkla izlenebilmektedir.

3.8.31. Otomatik Yazılım İndirme

Otomatik yazılım indirme tekniklerini kullanan ajan yazılım, arka planda gizli ve çok yavaş bir şekilde bir yazılımın, hedef bilgisayara indirilmesini ve indirilen bu yazılımın kullanıcının haberi olmadan kurulmasını sağlar. Kullanıcı o ajan yazılıma ait bazı bileşenleri silerek kaldırdığında, eksik öğeleri tekrar indirerek ajan yazılımın bilgisayar kayıtlarının sürdürmesine de yol açması açısından tehlikeli yapılardır.

BOLUM-4

4 AÇIK KAYNAKLI AĞ GÜVENLİK ÇÖZÜMLERİ

4.1 Açık Kaynaklı İşletim Sistemi

İlk olarak taslak kullanım şekliyle 1969'da KenThompsontarafından AT&T Bell Labratuvarları'nda Assembly dilinde geliştirilerek UNIX adını aldı. 1971'de DennisRitchie tarafından C dilinde tekrar yazılmıştır.

C derleyicileri yardımıyla Unix, diğer bilgisayarlarda da çalışabilir hale getirildi. Bu çalışmalar sonucu bir çok üniversite UNIX kopyalarını alarak kendi çalışmalarında bulundu. 1980 lerde ana farklılıklar gösteren UNIX sürümleri ortaya çıkmıştır.[24]

Başlıca UNIX sürümleri; *BSD UNIX,* Solaris, OpenSolaris, Linux, HP-UX, AIX, Minix, SCO Unix, Sun OS Linux.

Günümüzün en popüler Unix işletim sistemi olan Linux'u 1991'de LinusTorvaldstarafından geliştirildi. 1996'da Linux 2,470,00 satır C ve 8000 satır assembler koduna ulaşmıştır. Birçok donanım üreticisi tarafından desteklenerek bir standart haline gelmiştir. Kendi içinde tasarım ve kullanım biçimi olarak piyasada kullanılan bir çok sürümü bulunmaktadır. Başlıcaları; SuSe, FreeBSD, Gentoo, Debian, RedHat, IstanbulX, Pardus, Centos,Turkuaz…

Gerçek hayatta Linux işletim sistemi ile üretilen sistem çözümlerinin başlıcaları şu şekilde özetlenebilir.

- •Güvenlik Duvarları (Iptables, PF, IPF)
- •E-Posta Sunucular(Qmail, Sendmail, Postfix, Exim…)
- •Web Sunucular(Apache…)
- •Dizin Sunucuları(OpenLDAP, SunOne)
- •DNS Sunucular(Bind, TinyDNS, DjbDNS)

Günümüzde Unix-Linux çözümlerini kullananılanYerler/Kurumlar; Üniversiteler, Ford, GSM operatörleri, Alcatel, Türk Telekom, Ses lisanslı telekom operatörleri, NASA, cep telefonu ve kol saati üreticileri, Mars'daki robot.[25]

4.2 Açık Kaynaklı Ağ Yönetim Araçları

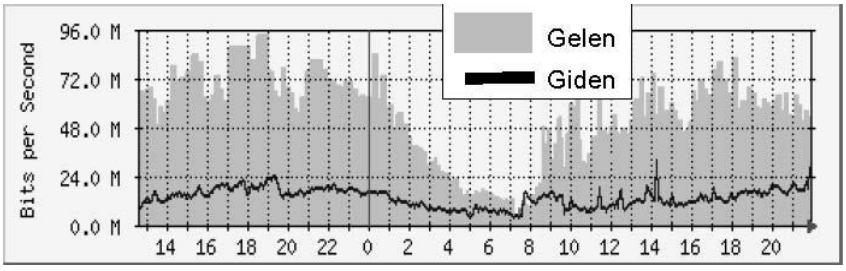
4.2.1 Linux Yönlendiriciler(Router)

TCP/IP ağların birleştirilmesini, kurumlar olarak ayrılıp tatnınmasını sağlayan yönlendiriciler, ağ yöneticileri için en önemli gözlem ve denetim noktalarıdır. Kaynakların paylaşılması açısından bakıldığında ağların birleştirilmesini sağlayan; ağ üzerindeki istenmeyen trafiğin yayılmasını önlemek açısından bakıldığında ise ağları birbirinden ayıran en önemli araçlar yönlendiricilerdir. Yönlendiriciler, marka ve modeli ne olursa olsun üzerinde TCP/IP yönlendirme ile ilgili yazılım(lar) çalışan, birden fazla arabirim üzerinden aynı anda birden fazla ağa bağlı olan, bu ağlar arası trafiği düzenleyen birer bilgisayardır.

Linux işletim sistemi ile kurulmuş bir bilgisayarı r yönlendirici olarak kullanılarak ticari yönlendiricilere göre herhangi bir işlev eksikliği olmadığı gibi birçok açıdan işlevsel ve yönetilebilirlik gibi üstünlükleride bulunmaktadır. Yönlendiricilerde genellikle çalışan yazılım *quagga* yönlendiriciler arasında ise OSPF *(Open Shortest Path First)* protokolu ile yönlendirme tablolarını birbirlerine ileterek topoloji değişikliklerine tam otomatik uyum sağlamaktadır. Yönlendiriciler üzerinde yerel ağ ekleme ya da çıkarma gibi değişiklikler yapıldığında kurulum temel ayarlarında değişiklik yapılmaz.

4.2.2 Ağ trafiğini izleme

Bir ağda neler olup bittiğini, ağ üzerinde akan trafiği ve bileşenlerini kritik noktalarda sürekli olarak ölçmek ve ölçülen bu değerleri daha önceki verilerle karşılaştırmaktır. Bu ölçümler yanlış giden birşeylerin varlığının tespiti yeni kaynak gereksinimlerin odaklandığı noktaların belirlenmesini sağlar. Kullanılan yazılım MRTG(Multi Router Traffic Grapher) yazılımıdır. Ağ üzerindeki noktalardan aktif cihazların SNMP protokolü ile toplanan verileri grafik olarak sunan ağ performans gözlem yazılımıdır. [26]



Şekil 4.2.2. MRTG grafiği veri akışı grafiğinden bir kesit

MRTG grafiklerdeki veri giriş-çıkışının günlük, haftalık aylık ve yıllık peryotlarda

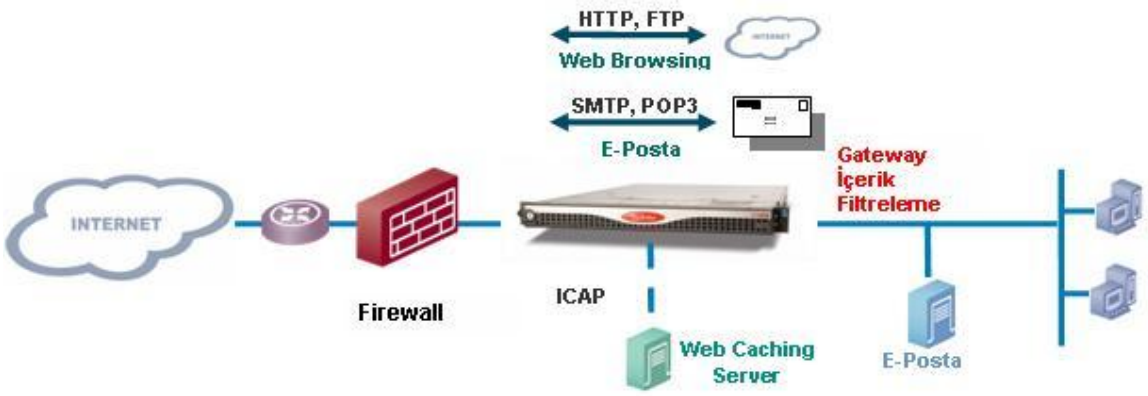
izlenebilmektedir. Ağda dışarı trafik oluşturan P2P(noktadan noktaya veri iletimi) görülebilmektedir. Özellikle yüksek boyutlu film ve ses paylaşımları bu şekilde tespit edilebilmektedir. Bu işlem için ağ içerisinde de NeTraMet yazılımı ile her bilgisayar için bu denetim sağlanabilmektedir. Yönlendirici arabirimlerindeki trafikleri gerçek zamanda ölçmek için kullanılan bir diğer önemli araç *iftop* yazılımıdır. Bu yazılımlada bilgisayarların gerçek zamanlı trafik yoğunluna bakılarak soluncan türü zararlı yazılımın varlığı tespit edilebilmektedir.

4.2.3 Trafik Denetimi

TCP/IP ağlarda trafik denetiminin yapılması için en uygun noktalar yönlendiricilerdir. Trafik denetimi için kullanılan yazılım, Linux çekirdeğinin bir parçası olarak çalışan *netfilter* ve bu yazılımın yönetim arayüzü olan *iptables* yazılımlarıdır. *netfilter/iptables* ile güvenlik duvarı (*firewall*), yük dengeleme (*load balancing*) ve trafik şekillendirme (*traffic shaping, QoS*) gibi işlevleri kolaylıkla ve etkin olarak yerine getirebilmektedir.

4.2.4 Güvenlik Duvarı (Firewall) İşlevleri

"Güvenlik duvarı" ya da "*firewall*" yazılımları tehlikeli ya da istenmeyen trafiğin bir bilgisayar ağına girmesini ya da çıkmasını önleyen denetim yazılımlarıdır. *netfilter/iptables* basit bir paket filtreleme yazılımının yanı sıra "Bağlantı izleme"(*connection tracking*) adı verilen özellik sayesinde basit paket filtresi olarakta çok büyük üstünlük sağlamaktadır. *iptables* ile gelen ve giden paketlerin durumuna karar verirken çıkış ve varış IP adresleri, port adresleri yanısıra paketlerin varış/çıkış sıklıkları, içerikleri, hatta günün tarih ve saatide dikkate alınabilmektedir. Örneğin deneme yanılmayla şifre kırma çabasının işareti olan, bir IP adresinden beş saniye içinde üçten fazla *ftp* ya da *ssh* bağlantı isteği geldiğinde, bu paketleri reddetmek ya da daha iyisi, görmezlikten gelmek olasıdır. Günümüzün sıkça kullanılan saldırı yöntemlerinden biri, http, smtp gibi servisleri aşırı yükleyerek sunucuları yanıt veremez hale getirmeye yönelik DoS (*Denial of Service*) saldırılarıdır. Bu saldırılarda, sunucu yazılımının yanıt veremeyeceği sıklıkta bağlantı isteği (SYN) gönderilir. *iptables* ile, gelen SYN paketlerinin sıklığını denetlemek aşırı yük oluşturan sıklıktaki paketleri durdurulabilir.



Şekil 4.2.4 Ağ üzerinde oluşturulan denetleyici durumdaki güvenlik duvarı

Şekilde 2.4.2'de oluşturulan bu yapı WEB protokolleri ve e-POSTA protokolleri üzerinden akan trafiğin zararlı içerikler bakımından denetlenmesidir**.** Bunlar virüs, spam, dolandırıcılık amaçlı elektronik postalar ve uygunsuz WEB sitelerine girişi engelleyen filtreleme fonksiyonlarının tamamını kapsayan bütünleşik çözümler olmalıdır. Ağ üzerinden geçen SMTP ve POP3 trafiğindeki zararlı kodlar kontrol edilmelidir. SMTP trafiği mutlaka spam kontroluna tabi tutulmalı ve merkezi olarak yönetilmelidir. Büyük ölçekli kurumlarda WEB (HTTP, FTP) ve e-POSTA (SMTP, POP3) trafiği sürekli taranıp temizlenmeldir.[15]

4.2.5 Yük Dengeleme / Sunucu Yedekleme

Yoğun kullanılan web uygulama sunucularında, SMTP sunucularında özellikle ağ trafiğinin denetlenmesinde performans sorunu yaşanabilir. Linux yönlendiricilerle *netfilter/iptables* yazılımı kullanılarak, bağlantı değerleri izlenerek, istemcilerden gelen paketler birden fazla sunucu arasında sırayla dağıtabilir. Örneğin bir web sitesini dört web sunucu üzerinde işletmek mümkündür. Dışarıdaki bir istemciden *http* bağlantı isteği geldiğinde, bu paket ve bu bağlantı ile ardından gelen ilgili tüm paketler, belirlenen kriterlere göre seçilecek bir sunucuya yönlendirilebilir.

Bir servisi birden fazla sunucu ile vermenin nedeni yedekleme amaçlıda olabilir. Sunucu yedekleme gerektiğinde kullanılabilen *keepalived* yazılımı hem ilgili sunucuları sürekli izlemekte, hem de bunlardan birinde bir aksaklık olduğunda yükü diğer sunucular arasında önceden belirlenmiş oranlarla paylaştırabilmektedir.

4.2.6 IP Adres Çoklama(NAT)

ADSL ve kablosuz ağ hizmetleri yaygınlaştıkça, NAT (*Network Address Translation*); bir

diğer deyişle, tek ya da az sayıda gerçek IP adresiyle çok sayıda bilgisayara ağ hizmeti verme gereksinimi de artmaktadır. NAT kullanmanın tek amacı IP adresinden tasarruf etmek değildir. Güvenlik amacıyla, kritik sunucuları ağiçindeözel IP adresleri ile gizleyerek dışarıdan gelebilecek saldırılara karşı korumak da yaygın olarak kullanılan bir NAT uygulamasıdır. *netfilter/iptables* yazılımının adres dönüştürme yeteneklerini, hem yük dağılımı yapmak hem de gelen tüm elektronik postaların önce bir virüs ve spam tarayıcı bilgisayardan geçirilmesini sağlamak amacıyla da kullanılabilir.

4.2.7 P2P ile Mücadele

Masaüstü bilgisayarların iyi denetlenemediği ağlarda P2P (Peertopeer) trafik çok ciddi bir sorun olmaktadır. Serbest bırakıldığında hat kapasitesinin tamamını tüketme eğilimindeki bu uygulamayı kontrol altına almak için *ipp2p* isimli *iptables* modülü kullanılabilir. ipp2p ile Kazaa, Ares, eDonkey, emule ve DC trafiklerini denetim altına alınmalıdır. *iptables* ile P2P paketlerini tamamen durdurulabildiği gibi filitreleme ve zararlı yazılımlara karşı tarama yapılabilir. Ayrıca ayrılan band genişliği de kısıtlanabilir.

4.2.8 Ağ Geçişini İzinlendirme

P2P dosya paylaşımı(BitTorrent gibi), web tabanlı dosya paylaşımı(RapidShare gibi), video paylaşımı(uTube gibi) band genişliğini hızla eriten uygulamalardır. Bunlar, özellikle üniversitelerde, yurtlarda ve ofislerde; günlerce, haftalarca aralıksız tam kapasite dosya indiren kullanıcılar diğer çalışmaları aksatacak boyutlarda trafik oluşturmaktadır. Bu tip gereksiz trafiklerin önüne geçebilmek için araya Proxy sunucu koyarak denetlenmelidir.

Şekil 4.2.8 Internet kullanımı izinlendirme ve kısıtlama

Proxy sunucu üzerine kurulacak açık kaynak kodlu *tc(traffic control)* yazılımı ile yönlendiriciler üzerinde değişik kapasitelerde birkaçband tanımlamak mümkündür.

Örneğin 100 Mbit bir hat üzerinde 60, 30 ve 10 Mbit'lik band genişlikleri tanımlanarak paylaşım sitelerinden dosya indiren kullanıcıların trafiğini 10 Mbit'lik banda; FTP, SMTP gibi zaman açısından fazla acil olmayan trafiği 30 Mbit'lik banda olarak paylaştırılabilir.[15]

4.2.9 Kablosuz Ağ Yönetimi

Hızla yaygınlaşan dizüstü bilgisayarlar kablosuz erişim isteklerini de beraberinde getirmektedir. Kablosuz erişim noktaları arttıkça yönettiğiniz ağa giren bilgisayarlar üzerinde denetimde azalıyor. Pek çok denetimsiz dizüstü bilgisayarın ağa girip çıkması virüs ve solucanların yayılmasını hızlandırmakta; ele geçirilmiş bilgisayarlar birer kablosuz Truva atı olarak ağda cirit atabilmektedir. Kablosuz bağlantı yapan kullanıcılar VPN (Virtual Private Network) protokolü ile erişimi sağlanabir. Kablosuz ağa bağlandıktan sonra geçerli bir kullanıcı kodu ve şifre vermeden kimse yönlendiricilerden geçemez. Bu sayede virüs, solucan, trojan yayan, ele geçirildiği için SPAM yollamaya çalışan bilgisayarların sahiplerinin kullandığı hesapları gerektiğinde bloke ederek denetim sağlanır. VPN bağlantıları için sunucu tarafında kullanılan yazılım, Linux'un standard servislerinden olan *pptpd* yazılımıdır.

4.3 Anti-Virus Çözümü

Virüsler ne yazık ki ağ yöneticilerinin birlikte yaşamayı ve başetmeyi öğrenmesi gereken önlenemez gerçeklerden biridir. Eposta ile yayılan virüsleri önleme konusunda açık kaynak kodlu yazılımlar kullanılmaktadır. e-posta sunucu üzerinde, açık kaynak kodlu *clamav* yazılımı ile tüm eposta mesajları üzerinde virüs taraması yapılır; temiz olan mesajlar ilgili kişilerin posta kutusuna yönlendirilir. *clamav* yazılımı belli saatlerde virüs veri tabanına bir ekleme olup olmadığını kontrol eder; varsa yeni virüs veri tabanını indirmektedir. *clamav* yaygın olarak kullanılan ve spam yakalama yeteneği oldukça güçlü olan bir yazılımdır.

Virüs ve solucan bulaşması sonucu ağ üzerinde sorun oluşturan bilgisayarların internet erişimi belli bir süre kesilerek bu bilgisayarları koruma tedbirleri aldıktan sonra tekrar erişimi sağlanmalıdır.

4.4 Solucanlarla Savaş

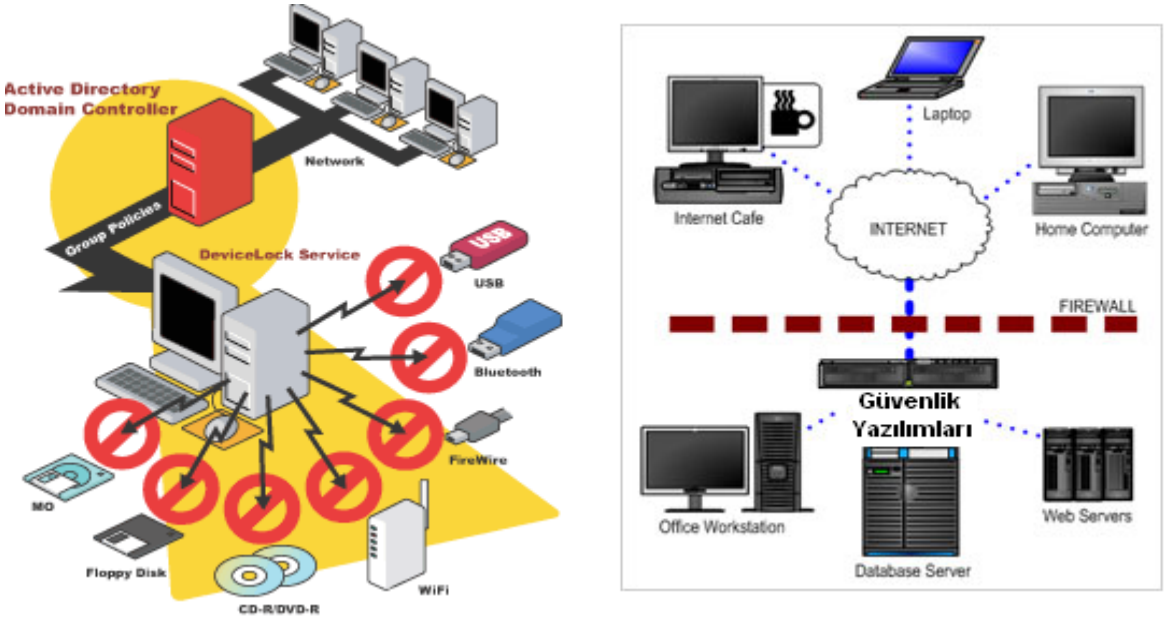
Solucan adı verilen yazılımların neredeyse tamamı Microsoft işletim sistemleri altında sunulan servislerin zayıflıklarından yararlanarak yayılmaktadır. Bu servislerin kullandığı

iletişim kapılarına (*port*) yönelik trafiği *iptables* ile denetim altına alarak solucan yayılımını önlemek mümkündür. İyi bir güvenlik duvarı kurulumunda bilinen port adresleri dışında trafiğe izin verilmez. Örneğin 135, 139 ve 445 numaralı portlar üzerindeki trafiğe denetimsiz olarak izin vermek kelimenin tek anlamıyla intihardır. Güvenlik duvarlarının politikası "herşey kapalı, gerekli olanlar açık" olmalıdır. *iptables* ile bu tür politikaları uygulamak son derece kolaydır. [27]

4.5 Anti-Spam Çözümü

2006 yılının sonlarına doğru artık dayanılmaz boyutlara varan istenmeyen eposta trafiği ile savaşta en önemli ve etkili çözüm açık kaynak kodlu yazılımlardır. Bu amaçla *spamassassin* açık kaynak kodlu yazılım ile birlikte kara liste servislerinden de yararlanılmalıdır. *spamassassin*, gelen eposta mesajlarının içerdikleri anahtar sözcükler yanısıra mesajın görsel düzenlenme karakteristiklerini (çok renkli yazı tipleri kullanılmış olması, "*listeden çıkmak için şunu yapın"* benzeri ifadeler içermesi gibi) değerlendirerek puanlama yapmakta; belirli bir puanı geçen mesajların SPAM olarak işaretlenmesini sağlamaktadır. DNSBL (DNS kara liste) servislerinden yararlanarak da, mesajı gönderen SMTP sunucunun şöhreti kontrol edilebilmektedir. *postfix*, *qmail*, *sendmail* gibi yaygın olarak kullanılan Linux eposta sunucu yazılımlarına kolaylıkla entegre edilebilen *spamassassin* SPAM mesajların yakalanmasında oldukça başarılıdır.

SPAM savaşındaki bir diğer önemli yazılımda *SQLgrey* isimli *grey listing* yazılımıdır. SPAM gönderen yazılımlar mesajları mümkün olduğunca hızlı göndermeye çalışırlar. Bunun en önemli nedeni, SPAM filtreleri yeniden düzenlenmeden olabildiğince çok mesaj göndermektir. Bu nedenle, gönderemedikleri mesajları bir süre sonra tekrar göndermeyi denemezler. *SQLgrey* yazılımı, herhangi bir IP adresinden herhangi bir kullanıcıya ilk kez gelen eposta mesajına ilişkin SMTP bağlantısını belli bir dakikalığına reddetmek. Eğer gönderici SMTP protokolunu kurallarına göre oynayan bir bilgisayarsa, kısa bir süre sonra tekrar deneyecektir. *Greylisting ile* gelen SPAM mesajların sayısında da azalma sağlanabilir. SPAM ile savaş tek yönlü değildir. Gelen SPAM'i önlemenin yanısıra, giden SPAM'in önlenmesi de kurumların kara listelere alınmaması açısından çok önemlidir. [28]



Şekil 4.5 Güvenlik açıkları ve açık kaynak kodlu yazılım denetim şeması

Şekil 4.5'de şeklin sol bölümünde görüldüğü gibi çok çeşitli yöntemlerle kullanıcı bilgisayarları ele geçirilmekte ve uzaktan yönetilerek SPAM göndermek amacıyla kullanılabilmektedir. Her ne kadar kuşkuyla karşılanan bir oran olsa da, dünyada Windows işletim sistemi ile çalışan ev bilgisayarlarının yüzdesinin büyük oranda ele geçirilmiştir. Microsoft çözüm olarak ağ üzerinde Active Directory Group Policies kullanıcı denetimini önermektedir. Sağ tarafta ise kurum hizmet sunucularının internet bulutundan ayrıldığı ve açık kaynaklı güvenlik firewall uygulamaları ile filitrelendiği yapıyı göstermektedir. Alınan tüm önlemlere rağmen, spam gönderen bilgisayarlara bakıldığında ağırlıklı iki tip olayla karşılşılmaktadır.

1. SPAM göndermek için uzaktan yönetilen, *zehirlenmiş(*ele geçirilmiş) bilgisayarlar

2. Kullanıcısının klavyede bastığı tüm tuşları, Windows ve MSN, ICQ gibi uygulama programları tarafından kaydedilen tüm kullanıcı kodu ve şifreleri bir yerlere eposta ile yollayan bilgisayarlar.

Bu bilgisayarlar incelendiğinde kullanıcılar genellikle, sohbet sitelerinde bir arkadaşları tarafından kendilerine tavsiye edilen ya da gönderilen bir programı kurduklarını veya "hoş" bir resim dosyasını açtıkları. Kullanıcıların kendi elleriyle, "*yalnızca bir kerecik*" yüklediği; üstelik "*böyle şeyler yapmayacak bir arkadaşından gelen"* bir yazılım nedeniyle bilgisayarının başkalarının denetimine geçtiği görülmektedir.

Bilgisayarlarınız ve ağlarınız ne kadar karışık olursa olsun, güvenlik açıklarından kaçınmak için sistemlerinizin her parçasının detaylarını düşünülmek zorunludur.

4.5.1 Anti-Spam Politikası Oluşturma

Bir kurumun *Kabul Edilebilir Kullanım Politikasında* (Acceptable Use Policy) kesinlikle spam'e karşı olunduğu ve öngörülen yaptırımlar belirtilmelidir. Böylece kullanıcılar önceden bilgilendirilmiş olacaktır.

SPAM ile savaşırken unutulmaması gereken en önemli kural spam'e karşı bir saldırı veya spam ile cevap vermenin herhangi bir yarar sağlamayacağı bilinmelidir. SPAM mesajların önlenmesi açısından sistem yöneticileri gerekli tedbirleri almalı Internet kullanıcıları ise bilinçlendirilmelidir.

İletiler yönetilen mail sunucusunun bir ara sunucu (relay) olarak kullanılması şeklinde iletiliyorsa, sunucuda relay özelliğini iptal etmek için gerekli ayarlamalar yapılmalıdır. SPAM iletilerinden korunmanın yollarından bir tanesi de, SPAM kaynağı veya açık relay olan mail sunucularının bir listesini kontrol etmek suretiyle, kara listedeki sunuculardan gelen mailleri reddetmektir.

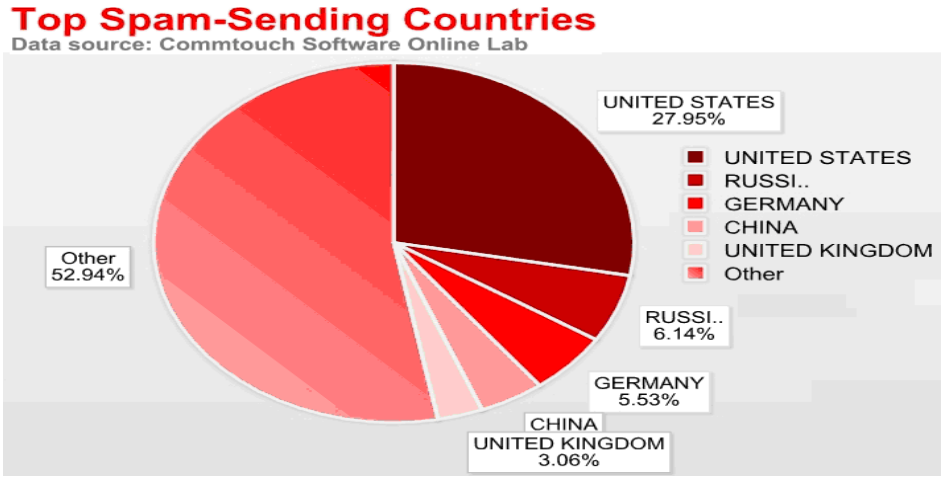
4.5.2 Karaliste Servislerinden Geçirme

Dünya üzerinde SPAM yayan sunucu ve ve IP'ler sürekli şikayet veya istatislik değerleri ne bakılarak tespit edilmektedir. Bunlar sürekli kendilerini gizleyerek farklı IP ve kuruluşlar üzerinden amaçlarına ulaşmaktadırlar. Bu tip karalisteleri güncel olarak tutan ve bu alanda faaliyet gösteren üç büyük servis bulunmaktadır. Bunlar;

MAPS – RBL (http://maps.vix.com/rbl): RBL (Realtime Blackhole List, Gerçek Zamanlı Karadelik Listesi) Mail Abuse Prevention Systems (MAPS) tarafından işletilmekte olan bir sistemdir. Serviste açık relay sunucuları olduğu kadar, sadece SPAM kaynağı olan sunucular da listelenir. TASO tarafından Türkiye kaynaklı spam iletilerini önlemek için ***RBL-TR*** adlı servis yürütülmektedir**.**

MAPS – RSS (http://maps.vix.com/rss): Relay Spam Stopper (RSS) servisi de MAPS tarafından işletilmektedir. RBL servisinden farklı olarak bu serviste, üzerinden spam gönderilen açık relay sunucular listelenir ve veritabanına yapılacak ekleme başvurularında SPAM ve açık relay'in kapatılması konusunda daha önce ilgili kuruma başvurulmuş olunması şartı aranmaz.

ORBS (http://www.orbs.org) : ORBS servisi RBL ve RSS'den farklı olarak sadece açık relay durumundaki sunucuları listeler. Sunucunun rapor edilmesi için sistem yöneticileri ile konu hakkında görüşülmüş olması gerekmediği gibi, sunucu üzerinden SPAM iletileri gönderiliyor olması da gerekmez.[29]



Şekil 4.5.2 Eylül 2007 itibariyle ülkelere göre spam dağılım oranları

Şekil 4.5.2 de açıkça görüleceği gibi internetin yoğun kullanıldığı ülkelerde spam dağılımıda yüksek oranda olmaktadır. Dünya genelinde karalisteye alınan IP bloklarıda dah çok bu ülkelere ait olmaktadır.

4.5.3 Karaliste Uygulama Modeli

Mail sunucularda "kara liste servisi" seçildiğinde varsayılan olarak MAPS-RBL servisi kullanıldığından en yaygın olan servistir. RBL servisi ile bir IP veya IP bloğundan gelen mail'ler tümüyle kapatılacağı için eğer karalisteye alınan bilinen belli bir adres ise doğrudan kapatmak sorunlara neden olabilir. Bu nedenle kullanıcının bu tür bir kapatma yöntemini uygulamadan önce ilk olarak spam gönderen site yöneticisine başvurmalıdır. IP bloğunun tümüyle kapatılabilmesi için, yapılan başvurunun olumsuz sonuçlanması veya kısa süre içerisinde yanıt alınamamış olması gerekmektedir. Cevap alınamıyorsa IP adresi yerine mail adresi veya domainin tamamı engellenmedir. Böylece o anda gelmeye devam eden istenmeyen mesajlar zaman kaybedilmeden engellenmektedir. Ayrıca ağ ve mail sunucuların kaynaklarının daha fazla israf edilmesinin önüne geçildiği gibi kullanıcıların da boşuna zaman harcaması engellenmektedir. İçerdeki kullanıcılardan gelebilecek spam adresleride bu sunucuda yer alan "spam veritabanı" na eklenerek spam mail'e karşı etkili önlem alınır. Spam'le savaşan kurumlar arası bir yardımlaşma ve dayanışma devamlılığı kurularak birbiriyle sürekli haberleşen sunucular bu karalisteleride kendi aralarında

güncellemelidir. Böylece kesintisiz olarak spam listelerini güncellemektedirler. Bu doğrultuda sisteme bağlı olan tüm sunucularda eş zamanlı olarak tüm spam gönderen mail adresleri engellenebilmektedir.

Rahatsızlık Nedeni	Kullanıcı Yüzdesi
SPAM'in istenmeyen bir şey olması	%84
Rahatsız edici çirkin içerik	%80
Bilgisayara zarar verme potansiyeli	%79
SPAM E-postaların yüksek boyutu	%77
Müstehcen içerik	%76
Gizlilik haklarına tecavüz	%76
Durdurulamıyor oluşu	%75
Zaman kaybettirmesi	%69

Tablo 4.5.3 Kara liste politikasının geçerliliğine yönelik çalışma

SPAM e-posta üzerine yapılmış bir araştırma sonucu spam'in son kullanıcı tarafında oluşturduğu rahatsızlığın boyutları hakkında bilgi vermektedir.

4.5.4 Güvenli Elektronik Haberleşme Konfigurasyonu

1. Kullanıcı tarafından konfigure edilebilir karalisteler(***black list)***'ler oluşturulabilmeli.

2. Kullanıcı tarafından düzenlenebilir özel izin verilecekler(***white list)'***ler (MS Outlook ve Qmail entegrasyonu ile) eklenebilmelidir.

3. Kullanıcı tarafından yönetilebilir karantina (Inbox'a geri besleme ve ***false positve'ler*** (Spam olmayan posta hatası, false positive oranı o kadar yüksek olur) için ***Bayesian filtreleme*** (Bayesian analizi, Spam postaların analizlerinden oluşan istatistikleri kullanarak kendi kendine öğrenir).

4. Bayesian Filtreleme için manuel öğrenme (Bayesian filtrelemeyi geliştirmeye yönelik false pozitifler için geri besleme mekanizması yapılabilmeli.

5. Puanlama sistemine dayalı anti-spam motoru ile entegre RBL (3. parti black list) desteği

6. ***Anti-Phishing*** filtreleme (***anti-fraud*** / dolandırıcılık, sahtekarlık amaçlı e-postalar)

7. Merkezi yönetim ve raporlama sistemi bulunmalıdır.

8. IMAP desteği (Internet Message Access Protocol) olmalıdır.

9. SPF desteği (envelope return-path authentication) SPF sınamaları yapan alıcı konaklar, taklit edilmiş adreslerle gönderilmiş postaları kabul etmeyecektir.

10. Posta Şifreleme / ***Encryption*** (TLS) ve SSL bağlantı olmalıdır.

11. ***Directory Harvesting*** ataklarından korunma (spamci SMTP protokolünün avantajlarını kullanarak, hedeflenen domain'e sürekli e-postalar gönderir birçoğu gerçek bir adresle

eşleşmemesine rağmen reddolmaz, saldırgan geçerli e-posta adresi bulana kadar devam eder(max. birkaç saat içerisinde gerçekleşir). Dünyada ortalama hergün 15.000 spam mail bu şekilde atak meydana getirmektedir. [30]

Şekil 4.5.4 Güvenli elektronik haberleşme yazılım bileşenleri

Yukardaki şekilde spamle mücadelede kullanılması gereken temel yazılımlar özetlenmiştir. İş dünyası başta olmak üzere akademik ortamlar ve kamu kurumlarında e-mail, doküman paylaşımı, hızlı ileti gün geçtikçe çok daha kritik altyapı bileşenleri haline gelmektedir. Kötü niyeti yazılım ve spam oluşturan kişiler, kurumsal ağlara girebilmek için birinci yöntem olarak e-posta sunucularını kullanılmaktadır. Örneğin MSN Hotmail tek başına günde yaklaşık 3 milyar spam iletisini taşımaktadır. Dolayısıyla spam sorunun üstesinden gelinebilmesi ve ağ güvenliği'nin sağlanması için bu yazılımlar mutlaka kullanılmalıdır. Gerek ağ üzerinde filtreler gerekse kişisel bilgisayralar ve sunucular üzerinde sıkı filitreler uygulayarak spamle mücadele de bütünlük ve süreklilik sağlanmalıdır.

Bilgisayar güvenliği ile ilgili olarak;

- E-mail alırken ve gönderirken e-mail eklentilerinden olabildiğince sakınılmalı.
- Asla e-mail eklentileriyle gelen ve uzantıları ".PIF, .EXE. .VBS" vb. dosyalar açılmamalı. Bu uzantılar çoğunlukla eklentilerde virüs taşırlar.
- Asla çift uzantılı eklentileri açmayın (NAME.BMP.EXE ya da NAME.TXT.VBS)
- Gerekli olmadıkça diğer kullanıcılarla dosyalarınızı paylaşmayın.
- e-mail farklı bir dille yazılmışsa iletiyi açmadan önce gelen adres incelenmelidir.
- Ekli dosyaların ikonlarına güvenilmemeli. Wormlar sık sık bilindik ikonların resimleri kullanılarak görünürler.
- IRC, ICQ ya da AOL mesajlaşma sistemlerini kullanırken yabancılardan gelen eklentileri asla kabul edilmemelidir.

BOLUM-5

5 AÇIK KAYNAK KODLU ANTI-SPAM UYGULAMA YAZILIMI

Açık kaynak kodlu yazılımlar kural tabanlı tanımlamaya daha müsait oldğundan dolayı spam taramada oldukça etkilidir. Örneğin spamassassin anti-spam yazılımı 800 den fazla kuralı içinde barındırmaktadır. Bu kurallara göre bir postanın spam olup olmadığına karar verebilir. Esnek ve gelişmiş programlama arabirimi sayesinde hemen hemen tüm posta sunucularla çalışabilen yazılımlardır. Bir çok Zaralı içerik ve eklenti taraması apabilen yazılımlar bir birleriyle uyumlu şekilde çalışabilmektedirler. Bunlardan başlıcaları spamasssin, Razor, Pyzor, Dcc gelir. [31]

Elektronik haberleşmede tam bir güvenlik sağlanılabilmesi için anti-spam, anti-virus, anti-trojan, anti-spayware gibi uygulamaların merkezi sunucularla taranarak son kullanıcıya ulaştırılması gerekmektedir.

5.1 Sunucu Güvenlik Yapılandırması

5.1.1 Antivirüs Modülü

Gelen ve giden tüm e-posta trafiği için taramalar aracılıyla ağ geçidi seviyelerinde antivirüs koruması sağlanmalıdır. Tam olarak gerçek zamanda mesajların yerel yada uzaktaki sunuculardan gelmelerini önemsemeksizin tüm SMTP trafiğini ağ geçidi üzerinden doğrudan taranmalıdır.

5.1.2 Karantina Modülü

Şüpheli dosyaları güvenli karantina bölgesinde izole edilerek ve yayılmadan dezenfekte edilmelidir. Karantina bölgesi belli zaman aralıklarında IT yöneticisi tarafından analizi yapılmalarak olası hataları gözlemlemelidir.

5.1.3 Antispam Modülü

E-postaların sunucu üzerinden aktarımı sırasında bazı filitrelerden geçirilir. Bunlar; Bayesian süzgeci, geliştirilmiş sezgisel süzgeç, White List/Black List ve URL süzgeci. Bu bileşenler düşük bir bellek alanı ile son derece hızlı tarama yapabilmektedir.

Sezgisel Süzgeç ile iletiler spamin karakteristiğine göre incelenir. WBL(White List/Blabclist) desteği ile, karaliste adreslerinden gelen e-postaları geri çevirirken, güvenli olarak belirtilen adreslerden gelenlere izin verecektir.

URL Süzgeci ile; bir çok spam mesajı genellikle çok sayıda reklam ve bir şeyler satın alabileceğiniz çeşitli türde farkı web konumlarına sahip bağlantılarla doludur. URL süzgeçlerine antispam verimine yardım edecek yeni bağlantılar eklenir veya silinir.

Bayesian Süzgeci; yalnızca bir tıklama ile kendi başına öğrenebilen gelişmiş iletilerinizi Spam ya da değil şeklinde sınıflamaya olanak sağlar. Süzgeç sadece bir kaç tekrarlama ile öğrenmeye başlar ve zaman geçtikçe daha yetenekli hale gelir. Yaplan her işaretleme süzgecin doğruluk oranını arttırır. Süzgecin duyarlılık ayarları istenildiği gibi yüksek yada alçak olarak ayarlanır. Spam sayısı eşik değerinden daha büyük ise mesajlar işaretlenir.

5.1.4 Akıllı Güncelleme

Virüslerin saptanması, tarama motorları ve antispam süzgeçleri için akıllı güncelleme yapılabilmelidir. Antivirüs korumasının akıllı güncelleştirmeleri kullanıcı müdehalesi gerektirmeden ağdan, internet üzerinden direkt olarak yada bir Proxy sunucusu aracılığı ile gerçekleştirilebilmelidir.

5.1.5 Akıllı Tarama

Birden fazla alıcıya gelen bir e-posta iletisi posta kutusuna teslim edilmeden önce süzülmelidir. E-posta alıcılarının dağıtım isteklerine ve e-postaların önem sırasına göre yeni tarama işlemleri organize edilebilmelidir.

5.1.6 Gelişmiş Rapor ve İstatistikler

Taranmış, dezenfekte edilmiş,silinmiş,virüslü yada süzülmüş mesajların,dosyaların yada nesnelerin numaralarına ilişkin otomatik raporlar üretilebilmelidir. Enfekte mesajlar yada alınmış saldırı niteliğindeki e-postalar hakkında posta yöneticisi bildirimler gönderebilmelidir.

5.1.7 Uzaktan Yönetim

Uzaktan yönetim antivirüs ve antispam korumalarını uzaktan yapılandırmak için bağımsız bir işletim sistemi şeklinde doğrudan tarayıcı yada atanmış konsoldan yapılabilmelidir. Yeni virüs belirlemelerde otomatik olarak erişebilmek, mevcut ağ seviyelerinde farklı tarama süreçleri başlatabilmek, şüpheli yada virüslü dosyaları silebilmek yada onarabilmek ve ağ olaylarının ayrıntılı raporlarını üretebilmek için uzaktan yapılandırılabilir olmalıdır.

5.1.8 Posta Başlıkları

Taranan, temizlenen ve şüpheli mesaj faliyetleri hakkında posta başlıklarına uyarlanabilir bilgi başlıklarını ekleyebilir yapı kurulmalıdır. Bunlara ek olarak mesaj altbilgileri ve virüs uyarıları şablon tabanlı IT personeli tarafından standart bir şirket tezkipi yada ihtiyaçları doğrultusunda değiştirebilecek şekilde düzenlenmelidir.

5.1.9 Diğer Modüller

Yukardaki modüllerin yanı sıra tüm internet üzerindeki yayılmış virüslere, spam faaliyetlerine ve malwarelere karşı zamanında ve verimli bir şekilde müdehale etmek için algılayıcılar bulunduran bir entegre yapı kurulmalıdır. OSI katman düzeyinde ve donanım ve yazılım güvenlik duvarlarıyla bu mimari desteklenmelidir.

5.1.10 Sistem gereksinimleri

Açık kaynak kodlu yazılımlar kullanılarak böylesi bir sistemin kurulabilmesi için donanım ve yazılım altyapısı aşağıdaki şekilde belirlenebilir.

- Minumum(Pentium III 500 Mhz işlemci, 40 GB disk, bellek alanı 256 MB RAM)
- Kernel v.2.2 veya v.2.4 olan Linux dağıtımları,
- RedHat Enterprise Linux: 2.1 , 3;
- SuSe Linux Enterprise Server 8,9;
- RedHat Linux: 7.x , 8.0 , 9 ;
- Fedora Core: 1 , 2 , 3;
- Debian GNU/Linux 3.x;
- SuSe Linux: 8.x , 9.x;
- Slackware: 8.x , 9.x , 10.x
- Mandrake: 8.x , 9.x , 10.x

5.2 Spamassassin İle Filitreleme

Spamassassin kural tabanlı açık kodla yazılmış bir spam önleme aracıdır. Spamassassin 800 den fazla kuralı içinde barındırır. Bu kurallara göre bir postanın spam olup olmadığına karar verebilir. Esnek ve gelişmiş programlama arabirimi sayesinde hemen hemen tüm posta sunucuları ile çalışabilr. Ayrıca birçok spam öneleme aracı ile de birlikte bir bütünlük içinde çalışabilir. Ayrıca RBL'leri (kara listeleri) kontrol edebilir ve MX kaydı sorgulaması yapabilir.

Çalışma mantığı kısaca, iletinin başlık bilgisi, konu kısmı ve iletinin gövde kısmı spam denetiminden geçiriliyor. Denetim sırasında her bir adım için puanlar veriliyor. Örneğin iletinin konu kısmı boşsa veya büyük harfler içeriyorsa, ileti gövdesi çok fazla HTML etiketi içeriyorsa ya da ileti birden çok kişiye gönderilmişse gibi kriterler gözönünde bulunduruluyor. Bir de bunlara RBL ve MX kontrolu ekleniyor. Bunların sonucunda yapılan puanlama bizim belirlediğimiz değere göre spam ya da değil şeklinde sonuçlanıyor.[32]

5.2.1 Spamassassin Kurulumu

Spamassassin, spam olarak nitelendirdiğimiz e-postaların tespit edilmesini, işaretlenmesini, ayıklanmasını sağlar.

Kurulum için http://spamassassin.apache.org/downloads.cgi adresinden en son sürümü indirilebilir. Paketler .tar.gz, .tar.bz2, .zip biçiminde olup tar paketlerini RPM haline getirdikten sonrada kurulum yapılabilir.

Kurulum için sistem üzerinde

- apt-get install spamassassin

komutu verilir. Kurulum sonrası ayarlar yapılması gerekmektedir. Bunu için;

http://www.yrex.com/spam/spamconfig.php adresinde konfigürasyon dosyasının oluşturulmasına yardımcı bir yazılım mevcuttur. Buradan istediğimiz özellikleri ve sınırlamaları belirtip kendi sistemimizde kullanabileceğimiz /etc/spamassassin/local.cf isimli konfigürasyon dosyamızı oluşturabiliriz.

Örnek /etc/spamassassin/local.cf :

```
#Bu dosya 3.x versiyonu için düzenlenmiştir.
#Kullandığınız Spamassassin versiyonuna ve sisteminizin durumuna göre dosyada
yapılması gereken değişiklikler olabilir.

# How many hits before a message is considered spam.
required_hits 5.0

# Text to prepend to subject if rewrite_subject is used
rewrite_header Subject ****SPAM(_SCORE_)****

# Encapsulate spam in an attachment
report_safe 1
```

```
# Enable the Bayes system
use_bayes 1

# Enable Bayes auto-learning
bayes_auto_learn 1

# Enable or disable network checks
skip_rbl_checks 0
use_razor2 1
use_pyzor 1

# Allows users to create rules
allow_user_rules 1

# Mail using languages used in these country codes will not be marked
# as being possibly spam in a foreign language.
ok_languages all

# Mail using locales used in these country codes will not be marked
# as being possibly spam in a foreign language.
ok_locales all
```

Şimdi ise sıra /etc/default/spamassassin dosyasının ayarlanmasına geldi,

/etc/default/spamassassin dosyasında

ENABLED=0 olan satırı

```
ENABLED=1
```

olarak değiştirelim. OPTIONS satırının da;

```
OPTIONS="--create-prefs --max-children 5 --helper-home-dir"
```

şeklinde olmasına dikkat edilmelidir.

Ayarların etkin olması ve spamassassin'in başlatılması için;

- /etc/init.d/spamassassin restart

komutunu vermemiz yeterlidir.

5.2.2 Spamassassin Ayarlarının Test Edilmesi

- spamassassin --lint

komutu ile /etc/spamassassin/local.cf dosyasında kabul görmeyen bir tanımlama yapıp yapmadığınızı görebilirsiniz. Dosyanın durumu ile ilgili daha detaylı bilgi edinmek için;

- spamassassin --lint -D

şeklinde bir komut ile daha detaylı bilgilere ulaşabilirsiniz. "-D" parametresi "debug" edebilmenizi sağlar.

5.2.3 Spamassassin'in Çalışma Yapısı

Spamassassin, gelen e-postaların durumlarına göre puanlar vererek, bizim **/etc/spamassassin/local.cf** dosyasında belirttiğimiz değeri (required_hits 5.0) aşan e-postaları SPAM olarak algılar. Şayet biz şu grubtan gelen e-postalar yada şu tarzdaki tüm e-

postalar SPAM olarak işaretlensin denilmişse, puan durumuna bakmadan doğrudan SPAM olarak algılar. Benzer şekilde, şu adresden gelen e-postaları kesinlikle spam olarak algılama dersek, bunların puanlarına bakmaksızın göz ardı eder.

Puanlama mantığı kabaca şu şekilde çalışır, subject (konu) kısmı boş olan e-postayı spam olma olasılığı sebebiyle, "spam puanı" veriyor olsun, yine söz konusu e-posta aynı anda birden fazla kişiye gönderilmişse yine spam olma olasılığının fazla olması ihtimaline binayen "spam puanı" veriyor olsun, e-posta içerisinde html tagları kullanılmışsa, çok süslü bir e-posta ise yine bununda spam olma olasılığı yüksek diyerek onada bir puanlama yapar. Benzer şekilde yaptığı puanlamaları toplayarak bizim **/etc/spamassassin/local.cf** de belirttiğimiz değeri (mesela, required_hits 5.0) aşan e-postaları, bu adresden gelen e-postalar veya benzer tarzdaki e-postalar için belirttiğimiz aksi bir başka kural olmadığı sürece SPAM olarak işaretler.[33]

Spam olarak işaretleme yaparken, istersek SPAM olarak algılanan e-postaların konu başlıklarının (subject) değiştirilmesini, var olan konu başlığının başına SPAM olduğunu belirten bir tag eklenmesini sağlayabiliriz. Bu işlemi gerçekleştiren kısım, **rewrite_header**' dır. Yukarıdaki dosyada spam olarak algılanan e-postaların konu başlıklarının başına "*******SPAM*******" ifadesinin de eklemesini söylemişiz bulunuyoruz. Bu kısımda gelen e-postanın kaç puan ile spam olarak işretlendiğini anlayabilmek için 3.x versiyonu ile birlikte "******SPAM(_SCORE_)******" şeklinde kullanabiliyoruz.

"**report_safe 1**" ifadesi ilede, kullanıcıya giden e-postalar, SPAM olarak algınırsa konu başlığı belirttiğimiz şekilde yeniden düzenlenecek ve mesajın orjinali mail'e Attach (ek) edilecek. Kullanıcı spam olan e-postayı direk göremeyecek, isterse söz konusu e-postanın ek dosyasından bakıp, bu e-postanın gerçekten spam olup olmadığına karar verebilir ve gereken işlemi yapabilir. Gelen e-posta spam olarak işaretlendiğinden direk sunucuda iken silinedebilir, fakat bu benim çok fazla tercih etmediğim bir yöntem. En azından sistemin düzgün işlediğine (ince ayarların yapıldığına) emin olmadan önce bu opsiyonu aktif etmek pek sağlıklı olmasa gerek, spam olmayan ama spam olarak algılanabilecek bir çok e-postayı kaybedebilirsiniz. Bunun yerine procmail veya maildrop kullanarak bu tarzdaki e-postaların akibetini "**.Spam**" klasörüne taşımak olarak belirtebiliriz.

5.2.4 Şüpheli E-postaların Spam Olarak İşaretlenmemesi

Belli domainlerden gelen e-postaların ne olursa olsun spam olarak işaretlenmemesi işlemi için,

/etc/spamassassin/local.cf dosyamızda bunları whitelist_from olarak belirtiyoruz. Örnekler:

```
whitelist_from *@isbank.com.tr
whitelist_from *@maximum.com.tr
```

```
whitelist_from *@akbank.com
```

yukarıdaki örneklerde garanti.com.tr, bonus.com.tr ve ykb.com dan gelecek e-postaları ne olursa olsun spam olarak işaretleme yada spam olarak algılama diyoruz.

5.2.5 Spam Olarak İşaretlenen E-postaların İçerisine Bilgi Mesajı Koyma

Yine, /etc/spamassassin/local.cf dosyamızı aşağıdaki şekilde düzenleyerek, kullanıcıya bilgi verebiliriz.

```
clear_report_template

report Bu Mail sunucusu üzerinde SPAM e-posları kontrol eden bir yazılım çalışmaktadır.
Bu yazılıma göre size gönderilmiş olan bu e-postanın SPAM içerebileceği tespit edilmiş ve
size gelen bu e-postanın orjinal hali (e-postanın SPAM OLMAMA ihtimaline karşı) -EK
DOSYA- olarak bu e-posta ile size gönderilmiştir.
report
report ----------------------------------------
report Bilgi için :: info@domainismi.com
report ----------------------------------------
```

gibi bir yapı ile , "**report**" ifadesini kullanarak kullanıcıya bilgilendirme mesajı gönderebilmiş oluyoruz.

5.2.6 Otomatik Öğrenme Metodu

Thomas Bayes tarafından bulunan, Bayesian metodu olarak bilinen bu yöntemi spamassassin içerisinde kullanarak otomatik öğrenmeyi sağlıyoruz. Kabaca ,o ana kadar gelen e-postaları değerlendirerek, gelen e-postalara göre daha sonraki e-postalarında spam olabilme olasılığını hesap eden bir metod. Metod gücünü, olasılık hesaplarından alıyor. Bu yöntemin aktif hale gelebilmesi için local.cf dosyamızda,

```
# Enable Bayes auto-learning
bayes_auto_learn 1
```

ayarlamasının yapılmış olmasına dikkat etmemiz gerekir.

5.2.7 E-postaların, Sisteme Kullanıcı Tarafından Öğretilmesi

sa-learn komutu ile gelen bir e-postanın benzerinin bir daha gelmesi durumunda spam olarak algılanmasını veya o tarz maillerin spam olarak algılanmamasını sağlayabiliriz.

- sa-learn --ham <epostaların_bulunduğu_dizin_ismi_veya_eposta_dosyası>

belirttiğimiz dizinde yer alan maillerin veya belirttiğimiz mail dosyasının, spam olarak algılanmamasını söyleyebiliriz. Benzer şekilde

- sa-learn --spam <epostaların_bulunduğu_dizin_ismi_veya_eposta_dosyası>

belirttiğimiz dizinde yer alan e-postaların veya belirttiğimiz e-posta dosyasının, spam olarak algılanmasını söyleyebiliriz.

Böylece biz, bu e-postayı veya bu tarzdaki e-postaları tanı, bundan sonra belirttiğim şekilde davran demiş oluyoruz.

5.2.8 Her Kullanıcıya Farklı Kuralların Uygulanması

Bu durumda kullanıcının e-posta dizininde oluşan (yoksa oluşturun) .spamassassin dizininin

içerisine "user_prefs" (~vpopmail/domain/kullanıcı_dizini/.spamassassin/user_prefs) diye bir dosya oluşturup, /etc/spamassassin/local.cf dosyasında belirttiğimiz kural setine benzer kuralları user_prefs içerisinde yapıyoruz.

5.2.9 Spam Olarak Algılanan E-postaların Farklı Bir Klasöre Taşınması

Burada devreye procmail veya maildrop giriyor (biz burada procmail üzerinde duracağız). Procmail kullanarak istediğiniz e-postaların istediğiniz işleme tabi tutulması işini rahatlıkla yapabilirsiniz. Bu konuda çok fazla detaya girmemekle beraber fikir vermesi açısından bir örnek .procmail dosyası vermek istiyorum. Konu ile ilgili detaylı anlatıma sahip bir çok döküman bulabilmek mümkün.

procmail'i sistemimize kurduktan sonra, kullanıcının ev dizininde procmail (~vpopmail/domain/kullanıcı_dizini/.procmail) isimli bir dosya oluşturup içerisine aşağıdakine benzer tanımlar yapabiliriz. Bu işlemin tüm kullanıcılara aynı anda etki etmesini istiyorsak /etc/procmailrc dosyasında işlem yapmamız gerekir.

Konu başlığında "*****SPAM*****" içeren e-postaları yok etmek için.

```
:0w
* ^Subject:.*\*\*\*\*\*SPAM\*\*\*\*\*\*
/dev/null
```

veya,

Konu başlığında "*****SPAM*****" içeren e-postaları aynı dizindeki .Spam/new/ dizinine aktarabiliriz. Bunun için de

```
:0w
* ^Subject:.*\*\*\*\*\*SPAM\*\*\*\*\*\*
./Spam/new
```

şeklinde bir kaç satır yeterli olacaktır.

5.3 Razor Kurulumu

Kullanıcılara daha önce gelmiş olan spam iletileri merkezi Razor sunucusuna bildirmesi ve daha sonra gelen iletilerin önceki iletilerle karşılaştırılması esasına göre çalışır. Spam iletilerin gövde karakteristikleri, daha sonra gelen iletilerle karşılaştırılmak üzere Razor sunucusunda depolanır. Üzerinde Razor kurulu olan posta sunucusu bir ileti aldığında bu iletiyi Razar sunucusundan sorgular. Eğer ileti Razor sunucusunda daha önce spam olarak kaydedilmişse, ileti spam olarak işaretlenir. SpamAssassin'le birlikte kullanıldığında başarısı %95'e kadar çıkmaktadır. Razor, spamassassin ile birlikte kullanılan ve spamassassin'in etkinliğini artıran bir yazılımdır. Aynı şekilde benzer görevi yapan Pyzor'u da sisteminize kurabilirsiniz. Aynı anda hem razor hemde pyzor kullanmak mümkün. Razor kurulumu için

- apt-get install razor

5.4 Pyzor Kurulumu

Pyzor'da esasen Razor'dan türemiş Python dili ile yazılmış GPL lisansına sahip bir yazılımdır. Veritabanı olarak Razor daha güçlüdür. Bu yazılımı kurarken sisteminize Python da kurulacaktır. Pyzor'un SpamAssassin'le birlikte çalışmasını sağlamak için /etc/mail/spamassassin/local.cf dosyasına aşağıdaki satırı eklemeliyiz:

use_pyzor 1

Bu yazılımıda sisteminize kurmak isterseniz,

- apt-get install pyzor

Pyzor 'un nasıl çalıştığını merak edenler http://www.archeus.plus.com/colin/pydoc/overview adresindeki kısa yazıya göz atabilirler. Bu yazı ile aynı zamanda Razor'un da çalışma mantığı anlaşılmış olacaktır.

5.5 Dcc Kurulumu

Sunucu/istemci tabanlı antispam aracıdır. Çalışma şekli Razor ve Pyzor'la aynı prensiplere dayanıyor. Alınan her ileti DCC sunucularındaki spam veritabanı ile karşılaştırılıyor. Sorgulama sonucuna göre iletinin spam olup olmadığına karar veriliyor. Razor ve Pyzor'la beraber aynı sunucda çalışabilir. Fakat unutulmamalı ki, tüm bu araçların aynı anda çalışması sunucu performansını ve internet bant genişliğini önemli ölçüde düşürür. Gelen herbir ileti için internetten bu uygulamaların sunucularına bağlanılacak ve sorgulama yapılacaktır. Genelde SpamasAssasin ile birlikte Razor kullanılmaktadır. Bu haliyle dahi başarı % 95 üzerinde gerçekleşmektedir. DCC sendmail ile doğrudan bütünleştirilebilir ya da ProcMail gibi bir eposta süzücü ile de çalıştırılabilir.

Benzer şekilde DCC'yi de kullanmak istersek;

- apt-get install dcc-common dcc-client

DCC'yi SpamAssassin ile birlikte çalıştırabilmek için /etc/mail/spamassassin/local.cf dosyasına şu satırı ekliyoruz.

```
use_dcc 1
```

DCC'nin **spamassassin**'le çalışmasını sınamak için

```
spamassassin --lint -D
```

komutu verilerek çıktısında DCC'nin sunucusuna bağlanabildiğini görülebilmelidir.

5.6 Razor Pyzor ve DCC'nin Spamassassin İle Kullanılması

Her iki yazılımında aktif olabilmesi için /etc/spamassassin/local.cf içerisinde

```
use_razor2 1
use_pyzor 1
use_dcc 1
```

ifadelerinin yer almasına dikkat edelim. Her üç yazılımıda aynı anda kullanabiliriz.

5.7 Maildrop Kurulumu

Spam olarak işaretlenen e-postaların hangi klasöre taşınacağını veya ne gibi bir işleme tabi tutulacağını belirtebilmek için kullanmamız gereken yazılım Maildrop veya procmail olabilir. Mesela kullanıcının e-posta dizininde .SPAM diye bir klasör oluşturup, SPAM olarak algılanan emaillerin bu klasöre taşınmasını sağlayabiliriz. Ayrıca qmail-scanner maildrop'a bağımlılık duyduğu için bu paketi kurmak durumundayız. Kurulum için

- apt-get install maildrop

5.8 Clam Antivirüs Kurulumu (Clamav)

Clam Antivirüs (Clamav) GPL lisansı ile dağıtılan bir yazılımdır.

- apt-get install clamav clamav-daemon

ile Clamav Antivirüs yazılımını sistemimize kurabiliriz.

"***Please choose the method for virus database updates***" kısmından uygun olan güncelleme metodonu seçiniz. sürekli internet bağlantısı olanlar için "**daemon**" uygun bir seçim olacaktır.

Sonraki adımda; "***new CA certificates will be trusted and installed***" seçeneğine "**Yes**" diyerek devam edelim.

Bunlarla birlikte önerilen paketlerden bazılarınıda kuralım

- apt-get install unrar-nonfree lha arj unzoo unzip daemon libcurl3-gssapi ca-certificates

İleriki adımlarda problem olacak slamav-daemon ile ilgili ayarları ayarları şimdiden yapalım. Qmailscanner için gerekli olacak olan qscand grubu ve kullanıcısını ekleyelim.

- groupadd qscand
- useradd -c "Qmail-Scanner Account" -g qscand -s /bin/false qscand

Daha sonra /etc/clamav/clamd.conf dosyasındaki;

"**User clamav**" ifadesini "**User qscand**" ile değiştirip clamd.conf dosyasını kaydediniz.

- chown qscand -R /var/run/clamav/

ile /var/run/clamav/ dizinine **qscand** kullanıcısının erişimini sağlayalım.

- /etc/init.d/clamav-daemon restart

ile clamav-daemon'u başlatabilirsiniz. İşlemleriniz yolunda ise /var/run/clamav/ içerisinde "**clamd.ctl**" dosyası oluşmuş olmalı.

5.9 Qmail-Scanner Kurulumu

Qmail-Scanner, Qmail için tasarlanmış içerik tarayıcı sistemidir. Clamav ve Spamassasin ile birlikte çalışması yararlıdır. Bu şekilde, sisteme gelen veya sistemden gönderilen maillerin kontrol edilmesini, virus içerip içermediğini veya spam olup olmadığını anlayabilmeyi sağlayacaktır. Bu yazılımın kurulumunuda yine .tar.gz 'den yapılır. Kurulum için,

Öncelikle sisteminizde yoksa qmail-scanner'in ihtiyaç duyduğu perl-suid paketini kurun,

- apt-get install perl-suid

daha sonra;

- cd /usr/local/src/
- wget http://unc.dl.sourceforge.net/sourceforge/qmail-scanner/qmail-scanner-1.25.tgz

(Son sürümünü, http://qmail-scanner.sourceforge.net adresinden kontrol ediniz.)

- tar -zxvf qmail-scanner-1.25.tgz

- cd qmail-scanner-1.25
- apt-get install unzip unrar-nonfree lha (kurulu değilse)

Aşağıdaki qscand grubu ve kullanıcısını clam-daemon ayarlarında eklenmelidir.

- groupadd qscand
- useradd -c "Qmail-Scanner Account" -g qscand -s /bin/false qscand

Koyu renkle işaretlenmiş yerlerde"**--admin *info* --domain *domainismi.com"*** ifadesi ile qmail-scanner.pl dosyasında admin'in mail adresinin ***info@domainismi.com*** olarak ayarlanması sağlanır. **"--notify *sender,admin,recips"*** ifadesi ile de, sisteme gelen/giden maillerin kontrolü sırasında Virüslü bir maile rastlanırsa, bunun ile ilgili bilginin maili gönderene (sender), sistem yöneticisine (admin, az önce belirttiğimiz mail adresine olmak üzere) ve mail alıcılarına (recips) bir rapor gönderilmesini, durumun iletilmesini sağlama işlemi yapılır. Şayet rapor'un (bilginin) sadece göndereciye gitmesini isterseniz bu kısımda "**--notify sender**" şeklinde düzenleme yapılabilir. Ayrıca qmail-scanner.pl dosyasındaki uyarı metinlerininde Türkçe olabilmesi için "**--lang tr_TR**" desteğine gerek vardır.

Şayet sistemde clamav'dan başka antivirüs programıda kullanılmak istenirse onuda **--scanners** ifadesinden sonra gelen "**clamdscan,verbose_spamassassin**" paremetreleri içerisinde belirtilmesi gerekir. Kullanılacak antivirüs yazılımının qmail-scanner tarafından destelendiğinden emin olmak gerekmektedir.

Clamav ile birlikte ikinci bir antivirus programı daha çalıştırmak istenirse **AntiVir** isimli antivirus yazılımın e-posa sunucuları için olan MailGate ürününü önerilebilir.

```
./configure --spooldir /var/spool/qmailscan --qmaildir
/var/qmail --bindir /var/qmail/bin --qmail-queue-binary
/var/qmail/bin/qmail-queue --admin info --domain domainismi.com --notify
sender,admin,recips --local-domains localhost --silent-viruses auto --lang tr_TR --debug 1
--unzip 1 --block-password-protected 0 --add-dscr-hdrs 1 --archive 0 --redundant no --log-
details yes --log-crypto 0 --fix-mime 1 --ignore-eol-check 0 --scanners
"clamdscan,verbose_spamassassin" --install 1
```

Kurulum sırasındaki bilgiler aşağıdakine benzer şekilde olacak.

```
Building Qmail-Scanner 1.25...
This script will search your system for the virus scanners it knows
about, and will ensure that all external programs
qmail-scanner-queue.pl uses are explicitly pathed for performance
reasons.
Continue? ([Y]/N) [Y ile devam ediyoruz]
The following binaries and scanners were found on your system:
mimeunpacker=/usr/bin/reformime
```

unzip=/usr/bin/unzip

Content/Virus Scanners installed on your System

clamscan=/usr/bin/clamscan

Qmail-Scanner details.

log-details=mailstats.csv
fix-mime=1
ignore-eol-check=0
debug=1
notify=**sender,admin,recips**
redundant-scanning=no
virus-admin=**info@domainismi.com**
local-domains='domainismi.com','localhost'
silent-viruses='klez','bugbear','hybris','yaha','braid','nimda','tanatos','sobig','winevar',
'palyh','fizzer','gibe','cailont', 'lovelorn','swen','dumaru','sober','hawawi','holar-
i','mimail','poffer','bagle', 'worm.galil','mydoom','worm.sco','tanx', 'novarg','\@mm'
scanners="clamscan_scanner"

If that looks correct, I will now generate qmail-scanner-queue.pl
for your system...
Continue? ([Y]/N) **[Burada Y ile devam ediyoruz]**

Hit RETURN to create initial directory structure under /var/spool/qmailscan,
and install qmail-scanner-queue.pl under /var/qmail/bin:
perlscanner: generate new DB file from /var/spool/qmailscan/quarantine-attachments.txt
perlscanner: total of 9 entries.

Finished installation of initial directory structure for Qmail-Scanner
under /var/spool/qmailscan and qmail-scanner-queue.pl under /var/qmail/bin.

Finished. Please read README(.html) and then go over the script
(/var/qmail/bin/qmail-scanner-queue.pl) to check paths/etc.

"/var/qmail/bin/qmail-scanner-queue.pl -r" should return some well-known virus
definitions to show that the internal perlscanner component is working.

That's it!

****** FINAL TEST ******

Please log into an unpriviledged account and run
/var/qmail/bin/qmail-scanner-queue.pl -g

If you see the error "Can't do setuid", or "Permission denied", then
refer to the FAQ.

(e.g. "setuidgid qmaild /var/qmail/bin/qmail-scanner-queue.pl -g")

That's it! To report success:

% (echo 'First M. Last'; cat SYSDEF)|mail jhaar-s4vstats@crom.trimble.co.nz
Replace First M. Last with your name.

Şeklinde kurulum tamamlanmış olacaktır. Şimdi "/var/qmail/bin/qmail-scanner-queue.pl -g" komutunu işleterek işlemi sonlandıralım.

- /var/qmail/bin/qmail-scanner-queue.pl -g
  perlscanner: generate new DB file from /var/spool/qmailscan/quarantine-attachments.txt
  perlscanner: total of 9 entries.

Bu işlemler sonucunda qmail-scanner-queue.pl dosyasının /var/qmail/bin/ altında yerini almış olması gerekir. Bu dosyanın hakları ile ilgilide, dosya sahibi ve grubunun qscand (qscand:qscand), chmod olarak erişim yetkisininde 4755 olarak ayarlanmış olmasına dikkat ediniz.

```
ls -al /var/qmail/bin/qmail-scanner-queue.pl
-rwsr-xr-x 1 qscand qscand 90980 2004-10-15 21:06 /var/qmail/bin/qmail-scanner-queue.pl
```

Ayrıca, /var/spool/qmailscan/ dizini yapısınında aşağıdakine benzer şekilde oluşturulmuş olup olmadığını kontrol ediniz.

```
ls -al /var/spool/qmailscan/
toplam 52
drwxrwx--- 5 qscand qscand 4096 2004-10-15 21:07 .
drwxr-xr-x 9 root root 4096 2004-10-15 21:06 ..
-rw-rw---- 1 qscand qscand 96 2004-10-15 21:06 mailstats.csv
-rw------- 1 qscand root 597 2004-10-15 21:06 qmail-queue.log
-rw------- 1 qscand root 18 2004-10-15 21:06 qmail-scanner-queue-version.txt
drwxrwx--- 5 qscand qscand 4096 2004-10-15 21:06 quarantine
-rw-r----- 1 qscand root 12288 2004-10-15 21:07 quarantine-attachments.db
-rw-rw---- 1 qscand qscand 4336 2004-10-15 21:06 quarantine-attachments.txt
-rw-rw---- 1 qscand qscand 0 2004-10-15 21:06 quarantine.log
drwx------ 2 qscand root 4096 2004-10-15 21:06 tmp
lrwxrwxrwx 1 qscand qscand 31 2004-10-15 21:06 viruses ->
/var/spool/qmailscan/quarantine
lrwxrwxrwx 1 qscand qscand 35 2004-10-15 21:06 viruses.log ->
/var/spool/qmailscan/quarantine.log
drwxrwx--- 5 qscand qscand 4096 2004-10-15 21:06 working
```

Şimdi /etc/tcp.smtp dosyasının Qmail-Scanner'ın devreye girebileceği şekilde düzenlenmesine geldi. /etc/tcp.smtp dosyasının içeriğini aşağıdaki şekile getirin.

```
127.0.0.1:allow,RELAYCLIENT="",QMAILQUEUE="/usr/sbin/qmail-scanner-queue.pl"
:allow,QMAILQUEUE="/usr/sbin/qmail-scanner-queue.pl"
```

Değişikliğin aktif olabilmesi için,

- tcprules /etc/tcp.smtp.cdb /etc/tcp.smtp.tmp < /etc/tcp.smtp

Şimdide, /var/qmail/bin/qmail-scanner-queue.pl dosyamızda aşağıdakine benzer şekilde olan satırların, aşağıdaki yapıda olup olmadığını kontrol edelim. Şayet ilgili satırlardaki tanımlar, bu şekilde değilse tanımları belirtilen şekile getirelim. Özellikle dikkat edilmesi gereken satırlar koyu renkle işaretlenmiştir.

```
my $clamscan_binary='/usr/bin/clamscan';
```

```
my $clamscan_options="-r -m --unzip --unrar --unzoo --lha --disable-summary --max-recursion=10 --max-space=100000";
my $clamdscan_binary='/usr/bin/clamdscan';
my $clamdscan_options="--no-summary";
my $spamc_binary='/usr/bin/spamc';
my $spamc_options=' -c ';
my $spamc_subject='';
my $spamassassin_binary='/usr/bin/spamassassin';
my ($sa_comment,$sa_level);
```

Evet, şimdi yazılımların kurulması ve yapılandırılması işlemi tamamlandı. Sistemimizi test etmek için,

- /etc/init.d/qmail restart

deyip, ilk önce qmailin düzgün şekilde başlayıp başlamadığını (telnet localhost 25) kontrol edelim. Benzer şekilde pop3 portunun aktif olup olmadığına (telnet localhost 110) bakalım. Bunlarda problem varsa, öncelikle /etc/init.d/qmail betiğinde yaptığımız ayarlarda sorun olmadığına emin olalım, daha sonra qmail-scanner ile ilgili ayarları gözden geçirelim.

5.10 Hataları Yakalamak ve Hatalarla Başa Çıkabilmek

- tail -f /var/log/mail.log
- tail -f /var/spool/qmailscan/qmail-queue.log

takip etmemiz gereken logların başında gelir. Özellikle /var/spool/qmailscan/qmail-queue.log dosyasında tutulan loglar sistemdeki sorunlar ve sorunların çözümüne ulaşabilmeniz için önemli ip uçları sunacaktır.

```
451 qq temporary problem (#4.3.0)
```

şeklinde veya aşağıdaki şekilde,

```
clamdscan: corrupt or unknown clamd scanner error or memory/resource/perms problem
```

hata alırsanız, /etc/init.d/qmail içerisindeki ulimit -v değerini artırıp qmail'i yeniden başlatıp kontrol edin. Örnek olarak bu değeri, "ulimit -v 65536" şeklinde bir değere ayarlayabilirsiniz (veya daha yüksek bir değere çekebilirsiniz). Bu değerin hemen aktif olabilmesi için bu ifadeyi komut satırından da işletebilirsiniz.

Ayrıca bu hataya sebep olabilecek olan, /etc/clamav/clamd.conf dosyasındaki "User clamav" ifadesinin "**User qscand**" olarak değiştirilmesine ve "**chown qscand -R /var/run/clamav**/" ile " /var/run/clamav/" dizininin qscand kullanıcısı içinde erişilebilir olmasına dikkat ediniz.

"/etc/init.d/clamav-daemon restart" komutunu işlettiğinizde "/var/run/clamav/" içerisinde "clamd.ctl" dosyasının yer alması gerektiğine dikkat ediniz.

Bu hatanın olası sebebi ile ilgili son olarak, "**perl-suid**" paketinin sistemde kurulu olduğuna emin olunuz.

5.11 Sistemin Komple Test Edilmesi

Sistemin çalışmasında bir sorun gözlemlemişseniz, sistemi genel olarak test edelim. Bunun için qmail-scanner içerisinden çıkan ufak betiği çalıştırıp genel bir fikir sahibi olabiliriz.

Yukarıdaki şekilde adımları takip etmişseniz qmail-scanner kaynak kodlarınız /usr/local/src/qmail-scanner-1.25/ dizininde bulunuyor olmalı. Bu dizin içerisindeki "contrib" isimli dizinde yer alan "**test_installation.sh**" isimli betiği aşağıdaki şekilde çalıştırarak spam ve viruslere karşı sistemimizin tutumuna bakabiliriz.[34]

- test_installation.sh -doit

Bunun yanısıra dilerseniz aşağıdaki şekilde gerekli testleri farklı şekillerde de yapabilirsiniz.

```
An error has occured.

Cannot find any reference to the Q-S administrator Email address in
/usr/sbin/qmail-scanner-queue.pl on your system!

Exiting....
```

Şeklinde bir hata mesajı ile işleminiz kesilirse "**/var/qmail/control/defaultdomain**" dosyasının içerisinde varsayılan olarak bulunmasını istediğiniz domaini belirtiniz. Bu dosya içerisine "**localhost**" gibi bir ifade de yazabilirsiniz.

"test_installation.sh -doit" işleminin sonucunda aşağıdakine benzer bir mesaj alacaksınız. Bu mesaj spam ve virüs testlerinin yapılıp sonucun qmail-scanner ayarlarında belirttiğiniz e-posta adresine gönderildiğini belirtiyor.

```
QMAILQUEUE was not set, defaulting to /var/qmail/bin/qmail-scanner-queue.pl for this
test...
QMAILQUEUE was not set, defaulting to /usr/sbin/qmail-scanner-queue.pl for this test...

Sending standard test message - no viruses...
done!

Sending eicar test virus - should be caught by perlscanner module...  done!

Sending eicar test virus with altered filename - should only be caught by commercial anti-
virus modules (if you have any)...

Sending bad spam message for anti-spam testing - In case you are using SpamAssassin...
Finished test. Now go and check Email for info@domainismi.com
```

5.11.1 Virus testi

Sisteminizi kontrol edebilmek için aşağıdaki adreslerden faydalanabilirsiniz.

http://www.webmail.us/testvirus

http://www.eicar.org/anti_virus_test_file.htm

http://www.webmail.us/testvirus

adresine e-posta adresinizi tanıtıp daha sonra ilgili adrese virüslü e-posta gönderebilirsiniz. Ayrıca http://www.eicar.org/anti_virus_test_file.htm adresinden indireceğiniz virüs içeren dosyayı kendinize göndererek benzer bir test de yapabilirsiniz.

5.11.2 Spam testi

- /usr/bin/spamassassin -t < /usr/share/doc/spamassassin/examples/sample-spam.txt

komutu ile /usr/share/doc/spamassassin/ dizininde yer alan sample-spam.txt dosyası ile Spam olan e-postalara karşı nasıl bir davranış göstereceği test edilebilir. Aynı şekilde,

- gunzip /usr/share/doc/spamassassin/examples/sample-nonspam.txt.gz
- /usr/bin/spamassassin -t < /usr/share/doc/spamassassin/examples/sample-nonspam.txt

komutu ilede spam olmayan e-postalara karşı nasıl bir davranış göstereceğini gözlemleyebiliriz.

Bu testler ile en azından sistemin çalışıp çalışmadığını öğrenebilirsiniz. Çalıştığına kanaat getirdikten sonra, en iyi sonuçlar için sisteminizi 1-2 gün gözlemleyerek duruma göre ayar dosyaları ile oynama yapabilir ve daha başarılı sonuçlar elde edebilirsiniz

5.12 Sistemin Sürekliliği ve Takibi

5.12.1 Squirrelmail'in attachment dosyalarının belirli aralıklarla temizlenmesi

Squirrelmail'in attachment dizini,

General Options -> Attachment Directory : /var/spool/squirrelmail/attach/

şeklinde "/usr/sbin/squirrelmail-configure" ile oluşturduğumuz ayar dosyasında tanımlanmıştır. Bu dizindeki (sizde farklı bir yeri gösteriyor olabilir) dosyaların belirli aralıklarla temizlenmesini sağlayabiliriz.

En son 3 gün önce erişilmiş dosyaları silmek için crontab içerisine aşağıdaki satırı uygun şekilde, uygun bir zamanda çalışacak şekilde ayarlayabilirsiniz.

```
Find /var/spool/squirrelmail/attach/ -type f -atime +3 | xargs rm -rf
```

5.12.2 Karantinaya alınan e-mail'lerin belirli aralıklarla temizlenmesi

En son 7 gün önce erişilmiş dosyaları silmek için crontab içerisine aşağıdaki satırı uygun şekilde, uygun bir zamanda çalışacak şekilde ayarlayabilirsiniz.

```
Find /var/spool/qmailscan/quarantine/new/ -type f -atime +7 | xargs rm -rf
```

5.12.3 Clamav'ın belirli aralıklarla güncellenmesi

Her 6 saatde bir güncellenmesi için crontaba aşağıdaki satırı yerleştirebilirsiniz.

```
* */6 * * * /usr/bin/freshclam /var/log/clam-update.log >/dev/null 2>&1
```

5.12.4 İstemcilerde (client) Smtp-Auth için gerekli ayar

Smtp-Auth, nasıl e-postalarımı sistemden çekerken, sistemin bizi tanıyabilmesi için kullanıcı adımızı (vpopmail ile oluşturduğumuz sistemde kullanıcı adı = email adresimiz olduğunu unutmayalım) ve şifremizi giriyoruz. Aynı şekilde Smtp-Auth destekli sistemler üzerinden e-posta gönderebilmek için, o sistemdeki kullanıcı adımız ve şifremiz ile doğrulama yapmamız gerekir.

Thunderbird, Kmail, Sylpheed, Evolution, Outlook gibi istemcilerde Smtp-Auth'u aktif edebilmek için "Sunucum Kimlik Doğrulaması Gerektirir" şeklindeki ifadenin yer aldığı ayarı aktif etmemiz gereklidir (gerekiyorsa, smtp-auth için kullanacağımız domain ismini, kullanıcı adımızı ve şifremizide bizden istenildiği şekilde ilgili yere girmemiz gerekir) .

NOT : Sistemde destek verilen Auth. tipini ("**telnet localhost 25**" dedikten sonra **EHLO** yazıp kontrol edilebilir.)

SONUÇ

Bilgi güvenliğine yönelik tehditlerin ciddi şekil ve nitelik değişimine uğradığı günümüzde, e-posta ve anlık mesajlaşma yoluyla gelen tehditlerin web uygulamalarınında ki açıklarla birleşmesiyle çok zararlı olabilecek saldırılarla karşı karşıyayız. Önemli kurumlarda dahi bilgi güvenliğinin ihmal edildiği, sonuçları ağır olabilecek şekilde özlük bilgileri, banka hesapları, ticari sırlar, e-posta gibi önemli ve hassas veriler internet ortamında yayınlanabilmektedir. Kullanıcıların önemli bir kısmı, saldırılara karşı yeterli korunma altında değildir. İşletim sistemi yama takipleri, dışarıdan gelecek saldırıları bertaraf edecek güvenlik duvarı ve antivirüs programlarının güncel kullanımı oldukça düşük seviyelerdedir. Kullanıcılar, İnternet'in tehlikeli bir ortam olduğunu ya bilgisayarları çöktüğünde, ya da kredi kartlarıyla alışveriş yapıldığında idrak etmektedir. En vahim durum ise İnternet bankacılığı bilgilerinin ele geçirilmesi ve hesaplarının boşaltılmasıdır.Web kaynaklı tehditler zararlı programların önemli bir kısmının yayılma yolu spam e-postalardır.

Spam e-posta girişimi ilk olarak, 1 Mayıs 1978 tarihinde DEC firmasının ABD'nin batı kıyısındaki tüm ARPANet adreslerine ürün tanıtımı gönderimi ile başlayıp her yıl %60-70 oranında artış göstermiştir. saldırı metodudur. Spam iletiler organize suç örgütlerinin işini kolaylaştıran, alıcı için bir şey ifade etmeyen, yalan ve yanıltıcı kişilik haklarını ihlal eden zararlı eklentilerin sığınağı olarak kullanılan e-postalardır. SPAM hareketinin merkezinde; aynı anda birden fazla kişiye gönderilen, başlık bilgileri tahrip edildiği için geriye dönük izlemesi hayli zor kullanıcı e-posta adresleri vardır. Bu toplu listeleri yasal olmayan yolla satın alarak yada arama motorları ile web sayfalarından taratılarak toplanmaktadır. SPAM iletiler yılda 20 milyar dolarlık finansal zarar, üretkenlik ve zaman kaybına neden olmaktadır. Ağ üzerinde ise; network trafiğini ve sunucu iş yüklerini beklenmedik oranda artırır, İnternetteki bağlantı süresini ve veri aktarım kapasitesini artırır. Kullanıcılar ve kurumlar SPAM ile mücadele için açık kaynak kodlu yazılım alternatiflerini tercih etmedikleri taktirde donanım ve yazılımlara para ödemek zorunda kalmaktadırlar.

İçeriği ürün-hizmet reklamı, ilaç/kozmatik ve sağlık ürünlerinin taklidi, illegal pornografi, hemen zengin ol/sahte para kazanma, saadet zinciri ve duygu sömrürüsü olan spam'ler e-posta iletişimini sağlayan altyapının %85'lik kısmı işgal etmektedir. Kullanıcılarında dikkatsizliği ve merakı neticesinde oluşan olumsuz bu durum karşısında e-posta hizmeti veren kurum ve servis sağlayıcıların özelikle sunucu odaklı bir takım önlemleri almaları

kaçınılmaz olmuştur. Ülkemizde bilgisayar ve İnternet kullanımı yaygınlaşıp, elektronik altyapı veri iletimi gerekliliklerinin üzerinde durulduğu bir zamanda, ağımızın ve değerli olan bilgilerimizin zarar görmemesi için kullanıcıların da spam ve diğer zararlı yazılımlarda bilgili bu konuda gerekli güvenlik önlemleri almaları gerekmektedir.

E-posta sunucusu ve kullanıcılar tarafında alınacak bazı güvenlik önlemleri;

- Yetkili posta sunucusu haricinde hiçbir bilgisayar dışarıya SMTP servisi vermemelidir.
- Ters DNS ve MX kaydı olmayan sunucuya posta servis izini verilmemelidir.
- Kullanılan işletim sistemleri, güvenlik yazılımları, web tarayıcıları ile e-posta istemcisi gibi internet yazılımları güncel olmalı ve güvenlik yamaları mutlaka kurulmalıdır.
- Ağ trafiği dinlenerek ani dalgalanmaların nedenleri rapor edilerek ve analizi yapılmalı.
- Daha az kaynak kullanılarak kuralların yeniden düzenlenip eklenebildiği açık kaynaklı IP tabanlı ve URL bazlı içerik filitreleme sistemleri kullanılmalıdır.
- Başka domainler adına posta göderimini engellemek için ilgili protokoller kapatılmalı.
- Açık kaynak kodlu güvenlik uygulamaları başta olmak üzere sunucu üzerinde, gelen-giden postaları tarayıp filitreden geçiren her türlü zararlı yazılımları bulup temizleyen ve yayılmasını önleyen, pop3,smtp ve http haricindeki tüm portları kapatan, son kullanıcıları merkezden kontrol eden firewall yazılımları kullanılmalıdır.
- Kişi ve kuruluşların e-posta adresleri, cep telefonu gibi kişiseldir outlook ve web uygulamalarında titizlikle korunmalıdır.
- Bir reklam ya da davetsiz bir e-mail alınırsa ekinde gelebilecek VBS, .SHS, EXE, VBS ya da .PIF benzeri dosyalar açılmamalı ve web linkleri kullanılmamalıdır.
- Haber gruplarından gelen dosyaları indirmekten ve yüklemekten sakınılmalıdır.

Sonuç olarak yukarıda belirtilen noktalardan da hareketle İnternetin oluşturduğu özgür iletişim ortamına zarar vermeden, bireysel ve ulusal kaynak israfına yol açmayacak şekilde her türlü güvenlik çözümleri süreklilik ve bütünlük içerisinde oluşturulmalıdır. Spam benzeri iletilerin yayılmasına vesile olabilecek her türlü güvenlik açıklarına karşı kullanıcılar bilinçlendirilmelidir. Spamle mücadelede güncelliğini kısa sürede kaybedebilecek ve sonu gelmeyen ticari yazılım ve donanım ürünleri yerine fazla sistem ihtiyacı gerektirmeyen verimli kaynak kullanımına sahip açık kaynaklı yazılımlarla milyonlarca dolar ulusal kaynak israfından tasarruf edilebilir. Tezin uygulama bölümünde anlatılan yapı üniversitemiz e-posta sunucuları üzerine uygulanmakta olup, 6.000 öğrencinin kullandığı e-posta iletişiminde başarılı şekilde kullanılmaktadır.

KAYNAKLAR

[1] http://www.gyte.edu.tr/Dosya//Bil472/Notlar1-3.pdf

[2] http://www.kou.edu.tr/idari/bilgiislem/ders/inttarih.htm

[3] http://www.denizliso.tobb.org.tr/ekol2/ekol/internet.html

[4] VALCOURT, S.A. 2003. 1st International Workshop on Community Networks and P/x Alphabet Soup: A Comparison of the Current State of DSL Technologies Managing Director, University of New Hampshire Interoperability Laboratory, New Hampshire, s14-15

[5] publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/cl/sndmsg.htm

[6] Scott Hazen Mueller, Eklemeler: Arif Oktay, Cev: C.Yucel)

[7] http://www.iss.net/x-force_report_images/2007/

[8] AUP (Kabuledilebilir Kullanım Politikası) Örnegi II : America Online, Çeviren : Deni Kanca, http://www.spam.org.tr/aup/aup2t.html

[9] Wi-Fi Alliance,Wi-Fi Protected Access:Strong, standards-based, interoperable security for today's Wi-Fi Networks,2003, Wi-Fi Alliance

[10] Baghaei N., 2003, IEEE 802.11 Wireless LAN Security Performance, Department of Computer Science and Software Engineering

[11] www.microsoft.com/Windows2000/downloads/servicepacks/sp2/loc/readme_tr.htm

[12] IDC August 2004, PM, and Raymond James Reporting

[13] http://www.turkattacker.org/index.php/topic,1433.0/wap2.html

[14] 2004 Hacker Raporu Gerçekten Güvenli Bir Pc İçin, CHİP, sayı.2004/04, Nisan 2004, pp.44-61.

[15] Serkan AKCAN - http://www.beyazsapka.org/yazi.aspx?id=9

[16] Spam Lab Online Statistics www.commtouch.com/site/Resources/statistics.asp

[17] Türk Hukuk Sitesi - www.turkhukuksitesi.com/showthread.php?t=11263 - 42k

[18] Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme, Canbek, G., Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Eylül 2005

[19] Politeknik Dergisi Cilt:10 Say_: 1 s. 33-39, 2007
http://www.politeknik.gazi.edu.tr/pdf_files/10133338.pdf

[20] Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri, Gürol Canbek, Şeref Sağıroğlu, Aralık 2006, Grafiker Yayıncılık, ISBN 975-6355-26-3

[21] Internet: Magid, L. J., "Child Safety on the Information Highway", National Center for Missing and Exploited Children (NCMEC) 2003.
http://www.safekids.com/child_safety.htm (16.05.2005).

[22] http://www.olympos.org/belgeler/linux-sunucu-guvenligi-ve-optimizasyon-ii-5343.html

[23] Kötücül ve Casus Yazılımlar - www.mmf.gazi.edu.tr/journal/2007

[24] http://www.enderunix.org/slides/KonyaSelcukUniversitesi/UnixIsletimSistemiAilesi.pdf

[25] Unix Basics; I450 Technology Seminar;Matt Hottell; 2003
http://www.forumturkiye.com

[26] Kampüs Ağ Yönetimi - csirt.ulakbim.gov.tr/dokumanlar/KampusAgYonetimi.pdf

[27] Linux Advanced Routing & Traffic Control, http://lartc.org

[28] http://www.ulakbim.gov.tr/dokumanlar/linux_ile_ag_yonetim_Calistay_2007.pdf

[29] Spam'den Korunma Çözümleri- www.spam.org.tr/rbl.html

[30] TBD Kamu-BIB – Bilisim Teknolojilerinin Hukuksal Boyutu, 15.05.2007

[31] http://www.lea-linux.org/cached/Postfix-courier-mysql-quota-spamassassin-amavis.html

[32] www.belgeler.org/howto/antispam-spamassasin.html

[33] Akademik Bilişim 2007 - ab.org.tr/ab07/bildiri/151.doc

[34] Qmail ve Vpopmail ile E-Posta Sistemi Oluşturulması - www.debian.org.tr

Yararlanılan Diğer İnternet Adresleri

http://belgeler.org

http://www.sorbs.net

http://www.sorbs.net

http://seminer.linux.org.tr

http://spamassassin.apache.org/

http://www.bayesian.org/bayesian/bayes.html

http://www.spam.org

http://mail-"abuse.org

http://www.orbl.org

http://www.ordb.org

http://www.beyazsapka.org

http://razor.sourceforge.net/

http://pyzor.sourceforge.net/

http://atrpms.net/dist/fc2/clamav/

http://www.clamav.net/

http://www.dazuko.org

http://www.eicar.org/

http://www.bayesian.org/bayesian/bayes.html