Gazi Üniv. Müh. Mim. Fak. Der.
Cilt 22, No 1, 121-136, 2007

J. Fac. Eng. Arch. Gazi Univ.
Vol 22, No 1, 121-136, 2007

KÖTÜCÜL VE CASUS YAZILIMLAR: KAPSAMLI BİR ARAŞTIRMA

Gürol CANBEK ve Şeref SAĞIROĞLU*
HAVELSAN A.Ş., Eskişehir yolu 7. km, 06520, Ankara
*Bilgisayar Mühendisliği Bölümü, Mühendislik-Mimarlık Fakültesi, Gazi Üniversitesi, Maltepe 06570, Ankara
gcanbek@havelsan.com.tr, ss@gazi.edu.tr

(Geliş/Received: 13.12.2005; Kabul/Accepted: 17.07.2006)

ÖZET

Bilgisayar teknolojileri gelişip yaygınlaştıkça, günlük iş ve işlemler elektronik ortamlara taşınmakta ve kolaylaşmaktadır. Bunun sonucu olarak bilgi ve bilgisayar güvenliğinin önemi ve karşılaşılan tehditler, gerek sayı gerekse çeşitlilik açısından artmıştır. Kötücül (malware) ve casus (spyware) yazılımlar ise bunların en başında gelmektedir. Bu yazılımlar ile ilgili olarak literatürdeki mevcut kaynaklar araştırılıp incelendiğinde, kapsamlı ve güncel bir çalışma olmadığı, sunulan çalışmaların ise anti-virüs web sitelerinde ve bilgisayar magazin dergilerinde yer aldığı ve nasıl korunması gerektiğiyle ilgili kısa bilgilere yer verildiği tespit edilmiştir. Bu tespitlerden yola çıkarak bu kapsamlı araştırma çalışmasında, en önemli tehditlerden olan kötücül ve casus yazılımlar üzerine kapsamlı bir inceleme gerçekleştirilmiştir. Elde edilen bulgular doğrultusunda, bu yazılımlar sınıflandırılmış; sahip oldukları temel özellikler ve taşıdıkları riskler özetlenmiştir. Bu çalışmanın, literatürde gerçekleştirilen kapsamlı bir çalışma olması sebebiyle, kötü niyetli olarak geliştirilen yazılım türlerinin daha iyi bilinmesi, tanınması ve gerekli önlemlerin alınmasına büyük katkılar sağlayacağı, karşılaşılabilecek zararların azaltılabileceği değerlendirilmektedir.

Anahtar Kelimeler: Kötücül yazılım, casus yazılım, bilgi ve bilgisayar güvenliği, virüs, solucan, arka kapı, Truva atı, kök kullanıcı takımı, klavye dinleme sistemi.

MALWARE AND SPYWARE: A COMPREHENSIVE REVIEW

ABSTRACT

As information technologies being developed and becoming widespread, daily routines and works have switched to electronic media and made life easier. As a result, the importance of information and computer security and threats encountered has increased in diversity as well as in quantity. New form of threats and attacks to security arise almost every day. Malware and spyware are very dangerous threats among them. Reviewing available literature on malicious software, it has not been found a well organized, up-to-date and comprehensive survey. When the literature reviewed, there have been a number of references covering from anti-virus web sites and computer magazines. In the light of reviewed literature, in this work, a comprehensive review on malware and spyware is classified and presented. This comprehensive work contributes to the computer users to know the threats of malicious software in details. The features of these wares and risks have been updated.

Keywords: Malware, spyware, information and computer security, virus, worm, backdoor, Trojan horse, rootkit, keylogger.

1. GİRİŞ (INTRODUCTION)

Bilgi güvenliği, bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme olarak tanımlanır. Bilgisayar teknolojilerinde güvenliğin amacı, kişi ve kurumların bu teknolojilerini kullanırken karşılaşabilecekleri tehdit ve tehlikelerin analizlerinin önceden yaparak gerekli önlemlerin alınmasıdır.

Bilgisayar teknolojilerinin gelişmesi ile son zamanlarda bilgi ve bilgisayar güvenliği konusunda en ciddi tehditlerin başında kötücül yazılımlar gelmektedir.

Kötücül 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 [1]. Kötücül yazılımlar, kullanıcının haberi olmadan veya kullanıcıyı yanıltarak sistemlere yetkisiz bir şekilde bulaşmaktadır [2].

Kirli yazılım (scumware) olarak da ifade edilen kötücül yazılımlar, hemen hemen her programlama veya betik (script) dili ile yazılabilmekte ya da birçok dosya içinde taşınabilmektedirler [3].

Tarihi gelişim açısından kötücül yazılımlar, dört kuşakta incelenebilir [2, 4]:

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

2. 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 kötücül 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.

3. Kuşak (1999–2002): Özellikle İnternet kullanımı ve e-posta iletişimin artması ile kitle postacılarının (mass mailer) arttığı bir dönemi kapsayan bu kuşakta, özellikle e-posta ve İnternet tarayıcı programlarında yer alan açıklardan istifade edilmektedir. Bu dönemde kötücül 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 kötücül yazılımlarının engellemesi ile belirli bir doyuma ulaşılmıştır.

4. Kuşak (2001–): Halen devam eden bu kuşağın diğer kuşaklardan en önemli farkı, yayılmak için belirgin bir kullanıcı yardımına ihtiyaç duymamasıdır. 2001'de Code Red solucanı ile başlayan bu dönemde, kötücül yazılımlar sistem ve programlarda bulunan korunmasızlıklardan yararlanmaktadır. Bu dönem ile özellikle yasadışı ve suç içeren sonuçlar doğuracak ve ciddi zarar veren kötücül yazılımlar yaygınlaşmaya başlamıştır. Bu kuşak ile beraber, klavye dinleme sistemleri gibi kendi kendini çoğaltmayan kötücül yazılımlar da ortaya çıkmıştır.

Şekil 1'de şema şeklinde gösterilen virüsler, solucanlar (worm), Truva atları (Trojan horse), arka kapılar (backdoor), mesaj sağanakları (spam), kök kullanıcı takımları

Şekil 1. Kötücül yazılım ana türleri (Main types of Malware)

(rootkit), telefon çeviriciler (dialer), korunmasızlık sömürücüleri (exploit), klavye dinleme sistemleri (keylogger), tarayıcı soyma (browser hijacking) ve casus yazılımlar (spyware) en genel kötücül yazılımlardır.

Sıradan kullanıcıları ve sistemleri tehdit eden kötücül yazılımlar, özellikle İnternet ve ağ sistemlerinin getirdiği hareket kolaylığı ile hızla yaygınlaşmaktadırlar [1]. Bu durum, iyi ve kötü adamların karşı karşıya geldiği teknolojik bir savaşa benzetilebilir. İnsanlar bu mücadele sırasında "kötücül yapıları" bulup temizlerken; verilerini, üretken olabilecekleri zamanlarını ve paralarını kayıp etmektedirler. Kötücül ve casus yazılımlardan korunma konusunda; araştırmacıların ve profesyonel güvenlik uzmanlarının bu tür zararlı öğeleri saptayıp, yeni yok etme yollarını geliştirmelerine; kullanıcıların eğitilip, bilinçlendirmesine; saptanan güvenlik boşluklarının kapatılmasına ve koruyucu, tarayıcı ve önleyici yazılımların kullanılması ve güncellenmesine rağmen, kötü niyetli kişilerin saldırıları ve saldırı yöntemleri her geçen gün artmaktadır [5].

Kötücül yazılımların etkileri konusunda son yıllarda yapılan inceleme çalışmaları, konunun ciddiyetini gözler önüne sermektedir [6-9]:

- "Code Red" solucanı İnternet üzerindeki korunmasız bilgisayarların hepsine 14 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).
- 2003 yılında TrendMicro'ya günlük rapor edilen yeni veya değiştirilmiş virüs tehdidi 20 ile 40 arasındadır (Reuters).
- Rasgele seçilen 300 firmadan 92'si 2003 yılında virüs saldırılardan dolayı büyük problemler yaşadı (25'den fazla bilgisayar etkilendi) (Computer Virus Prevalence Report).
- Geniş bant bağlantısı olan bilgisayarların yaklaşık %90'nında casus yazılım bulunduğu tahmin edilmektedir (Scott Culp, Microsoft).

- Casus 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 casus 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 [7]).
- Forrester'ın hazırlamış olduğu raporda, bilişim teknolojilerinde karar vericilerinin %40'ının, kötücül ve casus yazılımlar hakkında bilgilerinin olmadığı ve casus yazılımlardan etkilenip etkilenmediklerini bilmedikleri ortaya çıkmıştır (Forrester, 2005 [8]).
- Symantec, 2004 yılının ikinci yarısında 7360'dan fazla yeni kötücül yazılım tespit etmiştir. Bu sayının, 2004 yılı ikinci yarısından %64 oranında daha fazla olduğu açıklanmıştır (Symantec Internet Security Threat Report, 2005 [9]).

Yukarıda belirtilen hususlardan, bilgisayar kullanıcıların ve özellikle bilgi ve bilgisayar güvenliği uzmanlarının, bu önemli tehditleri tüm yönleriyle incelemeleri, tanımaları ve bilmeleri olaşabilecek ve karşılaşılabilecek zararların önüne geçmede yardımcı olacaktır.

Bu çalışmada, bilgisayar kullanıcılarının karşılaşabilecekleri tehdit ve tehlikeler incelenmiş ve bir tehdit gruplandırması yapılmıştır. En temel on bir farklı kötücül yazılım dışında, günümüzde daha birçok tehlikeli kötücül yazılım olduğu ve bu listenin genişletilmesi gerektiği görülmüştür.

Yapılan geniş araştırmalar sonucunda birçok kötücül yazılım tespit edilmiş; vermiş oldukları zararların büyüklüğü dikkate alınarak bu makalede 38 yeni kötücül yazılım incelenmiştir. Kötücül yazılımlarla ilgili bütün türler derlenmeye çalışılarak, varolan tehdidin tamamının gösterilmeye çalışılması, bu çalışmanın diğer hedeflerinden biridir.

Ayrıca, mantar gibi çoğalan kötücül yazılımları adlandırırken sonu "ware" ile biten oldukça fazla sayıda birbirinden ilginç İngilizce isim kullanılmaktadır. Bu çalışmada, bu tür terimlere Türkçe karşılıklar da önerilmiştir [1].

Bu çalışmada takip eden bölümler aşağıdaki şekilde düzenlenmiştir. Makalenin 2. bölümünde, öncelikle yukarıda bahsedilen on bir ana kötücül yazılım genel hatları ile açıklanmıştır. Bölüm 3'de ise birçok kaynaktan derlenen; fakat tamamı bir arada sunulmamış olan ve genelde çok az tanınan 38 yeni kötücül yazılım incelenmiş ve bu yazılımların en temel özellikleri verilmiştir. Son bölümde, kötücül ve casus yazılımlar genel hatları ile değerlendirilmiş; elde edilen sonuçlar sunulmuştur.

2. ANA KÖTÜCÜL YAZILIM TÜRLERİ (MAIN TYPES OF MALWARE)

Genel olarak tüm kötücül yazılımlar; yaşam döngüsü, kendi kendini çoğaltma, özerklik, bulaşma mekanizması, ayrık veya virüs özelliği taşıma, korunma mekanizması açısından farklı karakteristikler sergileyebilmektedir. Kötücül yazılımlar, yaşam döngüsünde her hangi bir aşamada farklı davranışlar sergileyebilecekleri gibi, kendi kendini çoğaltmayacak tek bir amaca yönelik çalışmakta; kullanıcının araya girmesine ihtiyaç duyabilecekleri gibi tamamen özerk bir yaklaşıma sahip olmakta; kötü niyetli kişiler tarafından bizzat elle hedef bilgisayar sistemine kurulabilmekte, kendisini saptayacak veya yok edecek korunma yapılarına karşı direnç gösterebilmekte, çeşitli taktiklerle bu tür programları atlatabilmektedir [2].

En temel kötücül yazılımlar, gelişme süreçleri açısından karşılaşılan ilk kötücül yazılım olmaları dışında; 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.

2.1. Bilgisayar Virüsleri (Computer Viruses)

Virüsler, en tehlikeli ve en eski kötücül yazılım olarak kabul edilmektedirler. Organizmalardaki hücrelere bulaşan küçük parçacıklar olarak tanımlanan biyolojik virüslerden esinlenerek adlandırılan bilgisayar virüsleri, kendi kopyalarını çalıştırılabilir diğer kodlara veya belgelere yerleştirilerek yayılan ve kendi kendine çoğalan programlardır. Ekranda rahatsız edici, çalışmaya kısa süreliğine de olsa mani olan mesajlar göstermek gibi zararsız sayılabilecek türlerinin de bulunmasına karşın, çoğu virüs programlarının, 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. Virüsleri diğer kötücül yazılımlardan ayıran en önemli özellik insan etkileşimine ihtiyaç duymasıdır. Virüs dâhilindeki kötücül kod mutlaka bir kullanıcı tarafından yürütülmelidir. Bir dosyanın açılmasıyla, bir e-postanın okunmasıyla, bir sistemi önyüklemesiyle (boot) veya virüs bulaşmış bir programı çalıştırması ile kullanıcı farkına varmadan virüsü yayar [10,11].

Virüsler yaygınlaştıkça virüs korunma programları da gelişmeye başlamış ve McAfee ve Symantec gibi firmaların öncülüğünü yaptığı virüs korunma programları, bilgisayar güvenlik sistemlerinin ayrılmaz parçası ol-

muştur. Bu firmalar, kötü niyetli kişiler tarafından geliştirilen "vahşi" (the wild) olarak tabir ettikleri virüslere karşı önlemler üretmek yanında; "hayvanat bahçesi" (zoo) ve "balçanağı" (honeypot) tabir ettikleri laboratuarlarında ileride çıkması muhtemel virüsler için de çeşitli çalışmalar yürütmektedirler.

Bilgisayar virüsleri;

- Dosya virüsleri
- Önyükleme (boot) virüsleri
- Makro virüsleri ve
- Betik (script) virüsler

olmak üzere dört sınıfta incelenebilirler. Dosya virüsleri, yayılmak için kendilerini çeşitli dizinlere kopyalayarak veya virütik kodlarını çalıştırılabilir dosyalara bulaştırarak, işletim sisteminde bulunan dosya sisteminde kullanan virüs türleridir.

Önyükleme (boot) virüsleri, sabit disk veya disketin "Ana Önyükleme Kaydını" (Master Boot Record) değiştirerek bilgisayarın her açılışında virütik kodun çalışmasını sağlayan virüslerdir. 26 Nisan 1986'da yaşanan Çernobil faciası üzerine Çernobil virüsü olarak adlandırılan ve bu tarihte bulaştığı konak sisteme zarar veren W95/CIH virüsü, önyükleme virüsleri arasında en çok tanınan ve oldukça zararlı virüslerden biridir [12].

Makro virüsleri, Microsoft Word ve Excel gibi güçlü makro desteği olan masaüstü programları kullanan ve bunlara ait belgelerin açılışında çalışan makrolar ile yayılan virüs türleridir. Çalıştırılabilir dosyalar dışındaki dosyalara bulaşan ilk virüs olan WinWord/Concept [13] ve Microsoft Excel çalışma sayfalarına bulaşan XM/Laroux, bu tür makro virüslerine örnek olarak verilebilir [5].

Betik (script) virüsleri, VB (Visual Basic), JavaScript, BAT (toplu işlem dosyası), PHP gibi betik dilleri kullanılarak yazılan virüslerdir. Bu virüsler ya diğer Windows veya Linux komut ve hizmet dosyalarına bulaşır ya da çok bileşenli virüslerin bir parçası olarak çalışırlar. Betik desteği olan ve zararsız gibi görünen HTML, Windows yardım (help) dosyaları, toplu işlem dosyaları ve Windows INF dosyaları, bu tür virüslerin yerleştiği dosyalar olarak karşımıza çıkabilir.

2.2. Bilgisayar Solucanları (Computer Worms)

Bilgisayar virüslerine benzer bir yapıda olan solucanlar, virüsler gibi bir başka çalıştırılabilir programa kendisini iliştirmez veya bu programın parçası olmazlar. Solucanlar, yayılmak için başka bir programa veya virüslerde olduğu gibi insan etkileşimine ihtiyaç duymayan, kendi kendini çoğaltan bir yapı arz ederler [14]. Bir solucanın yayılmasında kullandığı en yaygın yöntemler arasında, e-posta, FTP ve HTTP gibi İnternet hizmetleri bulunmaktadır. Solucanları yaymak için, hedef sistemdeki korunmasızlıklardan faydalanma veya kullanıcıların solucanları çalıştırabilmeleri için sosyal mühendislik yöntemlerini kullanma gibi yöntemler kullanılmaktadır. Solucanlar, başka dosyaları değiştirmezler; fakat etkin bir şekilde bellekte dururlar ve kendilerini kopyalarlar. Solucanlar otomatik olarak gerçekleştirilen ve genellikle kullanıcılara gözükmeyen işletim sistemi yapılarını kullanırlar. Solucanların kontrol dışı çoğalmaları, sistem kaynaklarını aşırı kullandığında veya diğer işlemekte olan görevleri yavaşlattığında veya bu görevlerin sonlanmalarına neden olduğunda farkına varılabilir. Solucan ismi, 1975 yılında John Brunner tarafından yazılan "Shockwave Rider" (Şok Dalgası Binicisi) adında bir bilim kurgu romanında, bir bilgisayar ağı üzerinden kendi kendini yayan bir programa verdiği isimden gelmektedir [15].

Bilgisayar solucanları; e-posta, IM (Internet Messaging), İnternet ve ağ solucanları olmak üzere dört grupta incelenebilir. E-posta solucanları, kötücül 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.

"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 mesajlar göndererek kendini yaymaya devam eder.

İnternet solucanları, sadece İnternet'e bağlı olan makinelere bulaşabilen solucanlardır. Bu tür solucanlar, İnternet üzerinde tarama yapar ve en son güvenlik güncellemelerini kurmamış olan, açık kapıları olan veya güvenlik duvarı olmayan korunmasız bilgisayarları bulmaya çalışırlar. Solucan böyle bir bilgisayar bulununca, kendini bu makineye kopyalar ve kendini kurar. W32/Blaster ve W32/Deloder bu tür solucanlara örnektir.

Bir başka ilginç solucan türü olan 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.

Çoğu solucan tek tip işletim sisteminde çalışacak şekilde geliştirilmektedir. Fakat çok yakın zamanda Windows, Linux, Solaris, BSD ve diğer işletim sistemlerinde çalışabilecek şekilde bir "savaş başlığı" içeren süper solucanlar ortaya çıkacaktır [11].

2.3. Truva Atları (Trojan Horses)

Yunan antik şairlerinden Homeros'un yazmış olduğu Odise adlı eserde: Yunanlıların Truva şehrini on sene boyunca kuşatmalarına rağmen şehri ele geçiremedikleri; bunun üzerine içine bir kaç düzine askerin saklandığı dev boyda bir atı hediye olarak kalenin içine sokmayı başardıkları ve gece geç vakitte at içinde saklanan askerlerin kalenin kapılarını içerden açarak şehrin ele geçirilmesini sağladıkları yazılmaktadır [16].

Tarihte birçok örneği görülen bu gizleme hilesini kullanan kötücül yazılımlar, bu efsanenin ismi ile anılmaktadır. Truva atları meşru yazılım gibi gözüken kötücül yazılımlardır. Son zamanlarda tersi de geçerli olan örnekler bulunsa da; Truva atları, virüsler gibi kendi kendine çoğalmayan yazılımlardır. Bir Truva atı faydalı bir 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, casusları, bildiriciler ve arşiv bombaları aşağıdaki türlerde Truva atları bulunmaktadır [17]:

Truva arka kapıları (Trojan backdoor): En yaygın ve tehlikeli Truva atı türüdür. Bulaştığı makinenin uzaktan kontrolünü sistem yöneticisinin farkına varmadan saldırgana veren araçlar içerir.

PSW Truva atları (PSW Trojan): Kişisel bilgisayarda bulunan şifreleri çalmak için kullanılan Truva atlarıdır.

Truva tıklayıcılar (Trojan clickers): İnternet tarayıcıların ayarlarını değiştirerek veya İnternet adresleri ile ilgili işletim sistemi dosyalarını değiştirerek hedef kullanıcının belirli bir siteye veya İnternet kaynağına yöneltmeyi 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.

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

Truva damlalıkları (Trojan droppers): Truva indiricileri gibi damlalıklar da başka bir kötücül yazılımın sisteme yerleşmesini sağlayan bir ara basamak vazifesi görür. Bu tür Truva atları içinde muziplik içeren bir dosyayı sadece sisteme yüklediğini hissettirerek programın sebep olduğu etkinliğin zararsız olduğunu düşündürür. Hâlbuki bu Truva atının asıl amacını yerine getiren diğer yükler için bir maskedir.

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

Truva casusları (Trojan spies): Tuş basımları, ekran görüntüleri, etkin uygulama kayıtları ve diğer kullanıcı faaliyetlerini toplayan ve bu bilgileri saldırgana gönderen Truva atlarıdır.

Truva bildiriciler (Trojan notifiers): 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.

Arşiv bombaları (ArcBombs): 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 giga baytlık bir veri RAR biçiminde 200 kilo bayta (ZIP biçiminde 408 kilo bayt) kadar sıkıştırılabilir. Yine 10100 adet eş dosya RAR biçiminde 20 kilo bayta (ZIP biçiminde 230 kilo bayta) kadar sıkıştırılabilir.

2.4. Casus Yazılımlar (Spyware)

Bilgi ve bilgisayar güvenliğinde casus yazılım, genelde muğlâk bir anlamda kullanılmaktadır. Casus yazılım, kullanıcılara ait önemli bilgilerin ve kullanıcının yaptığı işlemlerin, kullanıcının bilgisi olmadan toplanmasını ve bu bilgilerin kötü niyetli kişilere gönderilmesini sağlayan yazılım olarak tanımlanır. Bazı kaynaklarda dar manada "snoopware" (burun sokan yazılım) olarak da adlandırılan casus yazılımlar, diğer kötücül yazılımlara göre özellikle İnternet kullanıcıları tarafından sistemlere farkında olmadan bulaştırılmaktadırlar. Casus yazılımlar, virüs ve solucanlardan farklı olarak hedef sisteme bir kez bulaştıktan sonra kendi kopyasını oluşturarak daha fazla yayılmaya ihtiyaç duymazlar. Casus 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 [18]. Bunun dışında, ticari firmalar İnternet üzerindeki kullanıcı alışkanlıklarını saptamak amacıyla casus yazılımları İnternet üzerinde yayabilmektedirler [19]. Kullanıcıların haberi olmadan sistemlere bulaşabilen casus yazılımlar, kişisel

gizliliğe karşı gerçekleştirilen en önemli saldırılardan biridir [14].

Casus yazılımların sistemlere bulaşma teknikleri kullanıcılar tarafından çok iyi bilinmelidir. Bilgi ve bilgisayar güvenliğini sağlamada en önemli tedbirlerin başında gelen, bilgisayar sisteminin, yama ve güncellemelerle sürekli güncel tutulması ve İnternet üzerinde bilinmeyen programların indirilip, çalıştırılmaması gibi önlemler casus yazılımlara karşı da korunma sağlayacaktır. Bunun dışında nasıl virüslere karşı virüs korunma yazılımları kullanılıyorsa; son zamanlarda gelişme gösteren karşı casus yazılım (anti-spyware) ürünleri de bilgisayarların vazgeçilmez araçları olarak sistemlere kurulup en güncel halleri ile kullanılmalıdır. Çok sık rastlanan yanılgılardan biri de, virüs korunma programı bulunan bir bilgisayar sisteminin bütün kötücül ve casus yazılımlara karşı da korunma sağlayacağının sanılmasıdır. Virüs korunma programları elbette çok önemlidir ama bu çalışmada gözler önüne serildiği gibi sayısız kötücül ve casus yazılıma karşı ancak karşı casus yazılımlarla baş edilebilir.

2.5. 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 kötücül 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 olarak karşımıza çıkmaktadır. Bu durumun bir şekilde farkına varan kötü niyetli kişiler, bu yapıları kullanabilirler. Hatta bu tip arka kapılar bazen programcı tarafından kasten bırakılabilmektedir [21].

Arka kapı konusunda en ünlü iddialardan biri de Microsoft'un, Windows işletim sisteminin bütün sürümlerinde NSA (Amerikan National Security Agency) için bir arka kapı yerleştirdiği iddiasıdır. Bu iddia, Microsoft'un bütün sürümlerinde bulunan CryptoAPI yapısında, _NSAKey adına ilave bir giriş anahtarın bulunmasıdır [22].

2.6. Mesaj Sağanakları (Spams)

Mesaj sağanakları (spam, junkmail), belki de kullanıcıların günlük hayatta en sık karşılaştıkları ve sıkıntı çektikleri kötücül 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 [24]. 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.

2.7. Klavye Dinleme Sistemleri (Keyloggers)

Ortaya çıkan ilk türleri açısından ve en temel işlevi bakımından, kullanıcının klavye kullanarak girdiği bilgileri yakalayıp, tutan ve bunları saldırgana gönderen casus yazılımlardır. Klavye dinleme sistemlerinin son derece tehlikeli sonuçlar doğuracak kötücül amaçlarla kullanımı dışında, oldukça faydalı kullanım alanları da mevcuttur [1]. En etkili bilgi edinme yöntemlerinden biri olan klavye dinleme sistemleri aslında 1980'li yıllardan itibaren kullanılmaktadır [25]. Fakat bu konuda özellikle ülkemizde son zamanlarda bu konuda araştırmalar yapılmaya başlanmıştır [1]. Kötücül ve casus yazılımlara karşı hazırlanan paket programların çoğu, klavye dinleme sistemlerini dikkate almamaktadırlar. Bu yüzden kullanıcıların bu tür yapılara yönelik kendi tedbirlerini almaları veya klavye dinleme önleme sistemleri kullanmaları gereklidir.

2.8. Tarayıcı Soyma (Browser Hijacking)

URL zerki (URL injection) olarak da adlandırılan tarayıcı soyma, İnternet tarayıcı ayarlarını her zaman veya sadece belirli bölgeler için, kullanıcının belirlediği tarzın dışında davranmasına yol açan yazılımlardır [26]. Bu, en basit olarak, tarayıcı açıldığında gösterilen başlangıç sayfasını (home page), istenilen sitenin adresi yapmak olabilir. Bunun dışında uygunsuz içerik veya reklâm içeren çıkıveren pencereler (pop-up window) gösteren tarayıcı soyma türleri de bulunmaktadır [11].

2.9. Telefon Çeviriciler (Dialers)

Telefon çeviriciler, kurbanlarına büyük miktarlarda telefon ücreti ödetmek amacıyla, genellikle milletler arası uzak mesafe telefon numaralarını, hedef bilgisayar modeminin İnternet servis sağlayıcısının bağlantı numarası ile değiştirirler. Her zaman yaptığı gibi İnternet'e bağlanan kişi, aslında farklı bir hattı kullandığının geç farkına vardığında, çok büyük miktarlarda telefon faturası ile karşılaşabilir. Bazı telefon çeviriciler ise, tuş basım bilgilerini ve şifre gibi önemli bilgileri, kullanıcı belli bir süre aktif olmadığı bir anda, korsana telefon hattı kullanarak gönderirler. Son zamanlarda İnternet sitelerinde rastlanan kandırmacalardan biri de, belirli bir siteye erişmek için kullanıcının hazırlanan bir telefon çeviricisini kullanması gerektiğinin belirtilmesidir. Bu tür programlar asla indirilip, kurulmamalıdır [27].

2.10. Kök Kullanıcı Takımları (Rootkit)

UNIX işletim sistemlerinde yönetici anlamına gelen "root" isminden gelen kök kullanıcı takımları, saldırganın bir sistemin kontrolünü ele geçirdikten sonra, bilgisayar sistemine eklenen yazılımlardır. Takımda yer alan araçlar arasında, kayıt (log) girdilerini silerek veya saldırgan proseslerini gizleyerek, saldırının izlerini temizleyen araçlar ve saldırganın sisteme daha sonraki girişlerini kolaylaştıracak arka kapıları düzenleyen araçları sayabiliriz. UNIX işletim sisteminde bulunan netstat, ps, ls, du, ifconfig ve login gibi komut programlarının orijinalleri yerine geçen ve asıl işlevleri dışında korsana farklı imkânlar sunabilen kök kullanıcı takımındaki programlar, orijinalleri ile aynı sağlama toplamına (checksum) sahip olacak şekilde düzenlendiğinden; bu programların orijinallerinden farklı olduğunu anlamak sadece kriptografik özet karşılaştırması yapabilen "tripwire" ismi verilen bütünlük tarama programları ile mümkün olabilmektedir [20, 28]. ps komutu saldırgana ait kötücül prosesleri saklamak için; ls komutu gizlenmesi gereken dosya ve dizinleri saklamak için; du komutu saldırgan program ve kök kullanıcı takımları tarafından kullanılan disk alanını saklamak için değiştirilmektedir [29]. Çekirdek seviyesinde kök kullanıcı takımları, işletim sistemine çekirdek (kernel) seviyesinde çengel (hook) attıklarından, fark edilmeleri oldukça güçtür. UNIX ve türevi işletim sistemleri dışında Windows 2000 ve NT sistemleri için de kök kullanıcı takımları İnternet üzerinde rahatlıkla elde edilebilmektedir [18].

2.11. Korunmasızlık Sömürücüleri (Exploits)

Belirli bir güvenlik korunmasızlığını hedef alan türde saldırılar üretebilen kötücül yazılımlardır. Bu tür yazılımlar sadece bu korunmasızlığın varlığını bütün dünyaya göstermek amacıyla yazıldığı gibi; ağ solucanları gibi zararlı programların bulaşma yöntemi olarak da kullanılabilirler. Bir açıdan bakıldığında korunmasızlık sömürücüleri, ilgili olduğu işletim sistemini veya programı üreten firmanın bu tür açıkları kapatmak için harekete geçirten bir etkendir [30]. Korunmasızlık sömürücülerini en aza indirgemek için işletim sistemi ve programların bu tür açıkları oluşturmayacak şekilde geliştirilip, test edilmesi gereklidir.

3. GÜNCEL KÖTÜCÜL YAZILIMLAR (UP-TO-DATE MALWARE)

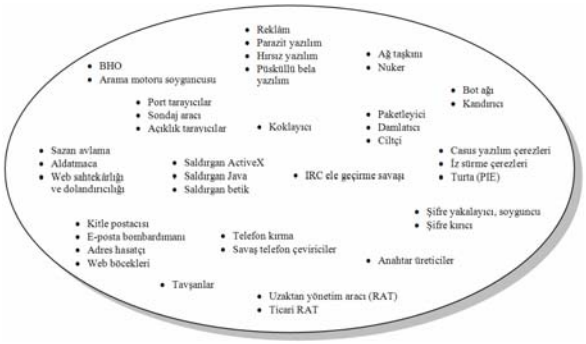
Yukarıda açıklanan kötücül yazılımlar dışında birçok kötücül yazılım türü bulunmaktadır. Bu yazılımlarla ilgili topluca ve yeterli sayıda kaynak ve çalışma bulunmamaktadır. Bu yazılımların sadece bir kaçından bahseden az sayıda kaynaklara İnternet üzerinde rastlanabilmektedir. Yeni nesil kötücül yazılımlar, teknolojinin getirdiği yenilikleri takip ederek ortaya çıkmakta veya şekil değiştirmektedir. Örneğin, ilk olarak Haziran 2004'de ortaya çıkan, EPOC.cabir ve Symbian/Cabir olarak da adlandırılan "Cabir" isimli bir bluetooth solucanı, Symbian işletim sisteminin bulunduğu cep telefonlarında da saldırı yapılabileceğini gösterdiğinden, cep telefonlarında da bilgi güvenliğine yönelik çalışmaların yapılması gerektiğini ortaya çıkarmıştır [31].

Güncel kötücül yazılımlar arasında, reklâm yazılım (adware), parazit yazılım (parasiteware), hırsız yazılım (thiefware), püsküllü bela yazılım (pestware), tarayıcı yardımcı nesnesi (Browser Helper Object, BHO), uzaktan yönetim aracı (Remote Administration Tool, RAT), ticari RAT (commercial RAT), bot ağı (botnet), ağ taşkını (flooder), saldırgan ActiveX (hostile ActiveX), saldırgan Java (hostile Java), saldırgan betik (hostile script), IRC ele geçirme savaşı (IRC takeover war), nuker, paketleyici (packer), ciltçi (binder), şifre yakalayıcılar (password capture) - şifre soyguncular (password hijacker), şifre kırıcılar (password cracker), anahtar üreticiler (key generator), e-posta bombalayıcı (mail bomber), kitle postacısı (mass mailer), e-posta adres hasatçısı (E-mail harvester), web böcekleri (web bugs), aldatmaca (hoax), sazan avlama (phishing), web sahtekârlığı (web scam) ve dolandırıcılığı (fraud), telefon kırma (phreaking, phone breaking), port tarayıcılar (port scanner), sondaj aracı (probe tool), arama motoru soyguncusu (search hijacker), koklayıcı (sniffer), kandırıcı (spoofer), casus yazılım çerezleri (spyware cookie), iz sürme çerezleri (tracking cookie), turta (PIE), damlatıcı (trickler), savaş telefon çeviricileri (war dialer) ve tavşanları (wabbit) saymak mümkündür. Bu yazılımlar aralarındaki yakınlıklara ve ilişkilere göre sınıflandırılmıştır. Yapılan bu sınıflandırma ise Şekil 2'de verilmiştir. Sınıflandırılan bu güncel kötücül yazılım türleri hakkında bilgiler ise aşağıda alt başlıklar halinde özetlenmiştir.

Var olan bütün kötücül yazılımları bu şekilde bir araya getirilerek sınıflandırılması resmin tamamını görmek ve eksiksiz bir güvenlik alt yapısı kurmak bakımından önemlidir.

3.1. Reklâm Yazılım (Adware)

Reklâm yazılımın kötücül yazılım olması şart değildir, fakat bu tür yazılımlar, bir bedava veya paylaşımlı



Şekil 2. Sınıflandırılmış kötücül yazılımlar (Classified Malware)

yazılımdan (freeware veya shareware) beklenebilecek reklâm anlayışının ötesinde yöntemler kullanırlar. Normalde yazılımlarda kullanılan reklâmların, 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. Kötücül yazılım olarak nitelendirilen reklâm yazılımlar ise, kullanıcıya reklâm yazılım ile beraber sunulan asıl programı çalıştırmasa da devrede olan programlardır.

3.2. Parazit Yazılım (Parasiteware)

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 açısından bakıldığında parazit yazılımlar, önemli bir güvenlik tehdidi olarak görülmez.

3.3. Hırsız Yazılım (Thiefware)

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].

3.4. Püsküllü Bela Yazılım (Pestware)

Reklâm yazılım türünde bir kötücül yazılımdır. Çoğunlukla ikiyüzlü üreticiler tarafından, kullanışlı bir program olarak sunulan ve kurulması önerilen yazılımlardır. Sisteme büyük zararlar vermeyen bu tür programlar, bilgisayar kullanımı sırasında verdikleri rahatsızlıklarla "püsküllü bela" olarak adlandırılabilecek, can sıkıcı bir hal alabilirler. Normalde bütün yazılım üreticileri, kurulan ürünü daha fazla kullanmak istemeyen kişilerin, programı sistemlerinden çıkartabilmeleri için bir program kaldırıcıyı (uninstaller) program menülerine ve/veya "Program Ekle/Kaldır" bölümüne eklerler. İşte püsküllü bela yazılımın en tipik belirtisi, programı diğer sıradan programlarda olduğu gibi otomatik olarak bilgisayardan kaldıracak bir yöntemin kasten sunulmamasıdır.

Püsküllü bela 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 koruyucuları ve daha iyi arama motoru sunma vaadinde bulunmaktadırlar [1]. Bir dereceye kadar vaatlerini yerine getirseler de; bu işe kendini adayan profesyonel programların daha ilerisine gidemeyen bu programların asıl amaçları, masaüstünüzde çeşitli şekillerde reklâmlar çıkartabilmektir. Belki bu reklâmların bir zararı olmayacağı düşünülse de bu yazılımların CPU, bellek ve bant genişliği gibi sistem kaynaklarını hoyratça kullandığı veya kullanım sırasında anormal sıkıntılarla günlük çalışma verimliliğini olumsuz yönde etkilemektedir.

3.5. Tarayıcı Yardımcı Nesnesi (Browser Helper Object, BHO)

İnternet Gezgini (Internet Explorer) her açıldığında otomatik olarak çalışan küçük programlar olarak üretilen BHO'lar, genel olarak tarayıcıya diğer yazılımlar tarafından yerleştirilir ve tipik olarak araç çubuğu donatıları tarafından kurulur. Kötücül amaçlarla yazılmış bir BHO nesnesi, İnternet tarayıcısına kurularak o kullanıcıya ait İnternet'te erişilen her bilgiyi toplayabilir ve kullanım verilerini gizlice izleyebilir [11].

3.6. Uzaktan Yönetim Aracı (Remote Administration Tool, RAT)

Saldırgana, hedef makine çevrim içi olduğu zaman bu makineye sınırsız erişim hakkı veren en tehlikeli kötücül 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 [5].

3.7. Ticari RAT (Commercial RAT)

Normalde uzaktan yönetim aracı olarak üretilen her hangi bir ticari RAT programının, kullanıcının izni veya bilgisi olmadan kötü amaçlarla kullanılmasıdır.

3.8. Bot Ağı (Botnet)

"Bot" terimi, bilgisayar teknik dilinde, özerk olarak çalışan ve bir kullanıcı veya program için, bir insan faaliyetini benzetmeye çalışan "yazılım robotlarının" yerine kullanılmaktadır. Örneğin, 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 yaygın bot'lar arasındadır [32]. Uzaktan yönetim yazılım türü olan bot ağı (botnet), kötü niyetli kişiler tarafından mesaj sağanağı (spam) göndermek, izinsiz daha fazla casus yazılım kurmak gibi kötü amaçlara yönelik kontrol altına aldıkları, bilgisayar solucanları ve Truva atları gibi kötücül yazılımların çalıştırıldığı, ele geçirilmiş bilgisayarlardan oluşmaktadır.

3.9. Ağ taşkını (Flooder)

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 taşkını saldırıları da bulunmaktadır [33].

3.10. Saldırgan ActiveX (Hostile 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 kötücül yazılımları indirip, kurabilir. Bazı saldırgan ActiveX yazılımları meşru ve imzalı ActiveX kontrollerinin adını kullanarak da, kötü niyetlerini saklayabilmektedirler [11].

3.11. Saldırgan Java (Hostile 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 [29]. Birçok güvenlik uzmanı bu durum karşısında, ya Java seçeneğini etkisiz kılmayı ya da daha ileri kum torbaları ve sanal makinelerle Java uygulamalarını sarmalamayı önermektedir.

3.12. Saldırgan Betik (Hostile Script)

.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 kötücül niyet açısından saldırgan betik olarak adlandırılmaktadır.

3.13. IRC Ele Geçirme Savaşı (IRC Takeover War)

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 oldukları yetki 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].

3.14. Nuker

Uygun şekilde yamalanmamış veya güvenlik duvarı olmayan 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 [35]. Ticari yazılımların yasal olmayan biçimde dağıtıldığı "warez" adı verilen bilgisayar dünyasında "Nuker", warez grubunun kurallara uymasını denetleyen kişilere verilen addır.

3.15. Paketleyici (Packer)

Bir prosesin içine bir dosyayı şifreleyerek sıkıştıran yardımcı programlardır. Program çalıştırıldığında, bellekteki dosyayı kendiliğinden açan bir başlığı prosese ekler [36]. Paketleyiciler, Truva atı geliştiricileri tarafından, çalışmalarının virüs korunma ürünleri tarafından saptanmasını önlemek için kullanılmaktadır.

3.16. Ciltçi (Binder)

Dosya yönetimi açısından ciltçi, Microsoft'un ciltçi yazılımı gibi, türleri farklı da olabilecek birden fazla dosyayı tek bir dosya haline getiren yazılımlardır. Fakat ne yazık ki bu tip dosyaların içine Truva atları gibi kötücül yazılımların da paketlenmesi mümkündür. Bu yüzden Microsoft dâhil birçok yazılım üreticisi, bu tip yazılımları üretmeyi bırakmışlardır [37].

3.17. Şifre Yakalayıcılar ve Şifre Soyguncular (Password Capture and Password Hijacker)

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

3.18. Şifre Kırıcılar (Password Cracker)

Kaba kuvvet ve sözlük tabanlı deneme yanılma yöntemlerini de içeren; bir şifreyi veya şifreli bir dosyanın şifresini çözen araçlardır [38,39]. 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 [40].

3.19. Anahtar Üreticiler (Key Generator)

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

3.20. E-posta Bombalayıcı (E-mail Bomber)

Hedef kişinin e-posta gelen kutusunu (inbox), binlerce e-posta ile bombardıman eden kötücül yazılımlardır. Gönderilen e-postalardan, gönderen kaynağın bilgisini elde etmek mümkün değildir [33].

3.21. Kitle Postacısı (Mass Mailer)

E-posta yolu ile virüs gönderen kötücül yazılımlardır. 1987'de yaşanan ilk CHRISTMA EXEC solucanı [41] ve 1999 yaşanan Melissa virüsü, bu tür kötücül yazılımlarla yayılmıştır [42].

3.22. E-posta Hasatçısı (E-mail Harvester)

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 bilgisayarlarda 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" e-posta adresi yem olarak kullanılabilir. Bu adrese gelen ilk e-posta iletisini gönderen kişinin, e-posta adres hasatçısı ile ilişkili olduğu iddia edilebilir [43].

3.23. Web Böcekleri (Web Bugs)

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 [44]. 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.

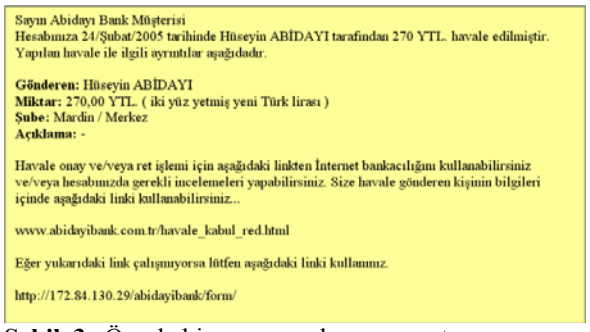
Web sayfaları ve e-postalar dışında Microsoft Word, Excel ve PowerPoint gibi ofis programı belgelerinde de web böceği uyarlamasının gerçekleştirilmesi mümkündür [45].

3.24. Aldatmaca (Hoax)

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 kötücül 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 [46]. 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, zararlı bir 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 [47].

3.25. Sazan Avlama (Phishing)

Dilimizde kullanılmak amacıyla "sazan avlama" olarak bir karşılık önerilen phishing, kimlik hırsızlığı (identity theft) adı verilen banka hesap numaraları, kredi kartı numaraları 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 [48]. Phishing için İngilizce "password harvesting fishing"in (şifre hasadı avcılığının) bir kısaltması olduğu ya da 1980'de ilk kez psikolojik teknikler kullanarak kredi kartı bilgilerini elde eden Brien Phish'e bir atıf olduğu belirtmektedir. 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 [49].


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

Şekil 3'te bir örneği gösterilen e-posta'ya benzer birçok mesaj, bugünlerde ülkemizde de insanlara gönderilmektedir [50]. 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.

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 bağlantıyı kullanan kişi sayfaya erişimde hata olduğuna dair bir uyarı alacaktır. Mesajda ek olarak verilen ve bahse konu bankanın sunucusunun değil de sazan avlamaya çıkan kötü niyetli kişinin sunucunun bulunduğu adres tuzak olarak verilmektedir. Bu adres, bölge adı şeklinde değil de, IP numarası (http://172.84.130.29) şeklinde, rakamlarla veriliyor. Burayı 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.

Mesajın, sazan avlama amacıyla kullanıldığını gösteren bu teknik bilgi dışında, aslında mesajın kendisi biraz dikkatlice incelendiğinde, mesajın kötü bir amaç için hazırlandığını gösteren birçok husus göze çarpmaktadır. Öncelikle kullanılan dil, profesyonel bir bankanın resmi üslubundan uzak dışındadır. Dilbilgisi ve noktalama hataları bulunan ve en önemlisi, mesajın gönderildiği kişinin tam adı yerine "Sayın Abidayı Bank Müşterisi" şeklinde genel bir ifade kullanılmaktadır.

Bu tür e-postalara karşı kullanıcılar bilinçli ve uyanık olmalıdır. Sazan avlamak isteyen kişilerin attıkları oltaya yem olunmamalı ve hiç bir şekilde kişisel bilgileri bu yolla isteyen mesajların söyledikleri yapılmamalıdır. Sazan avlamaya yönelik e-postalar, ilgili bankalara gönderilerek bankaların gerekli tedbirleri alması ve diğer müşterilerini bilinçlendirmesi sağlanmalıdır [1].

3.26. Web Sahtekârlığı ve Dolandırıcılığı (Web Scam and Fraud)

İnternet üzerinden veya e-posta ile yapılan bir dolandırıcılık türüdür. Genellikle İngilizce olarak yazılmasına karşın ileride ülkemizde de bu tür sahtekârlıklara rastlanacağı tahmin edilmektedir. Kişileri maddi veya manevi zararlara uğratacak türde etkileri olan ve İnternet üzerinde yapılan girişimler web sahtekârlığı olarak 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 [51].

3.27. Telefon Kırma (Phreaking, Phone Breaking)

1960'lı yıllardan beri elektronik yöntemlerle uygulanan telefon kırma, telefon dinleme, bedava telefon görüşmesi yapma amacıyla veya telefon şebeke ve santrallerine saldırı yapmak amacıyla, ses kartı ve modem kartı gibi donanımları kullanılan araçlara verilen addır [52,53].

3.28. Port Tarayıcılar (Port Scanner)

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.

3.29. Sondaj Aracı (Probe Tool)

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.

3.30. Arama Motoru Soyguncusu (Search Hijacker)

İnternet tarayıcıların varsayılan arama motoru ayarlarını değiştirmek amacıyla hazırlanan kötücül yazılımlardır. Bu şekilde arama yapmak isteyen kullanıcının sorguları veya olmayan veyahut yanlış girilen bir adres sonucu açılacak, varsayılan arama sayfası, başka bir siteye yönlendirilmektedir.

3.31. 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 ulaşılması istenen adrese yönlendirerek, koklayıcıların paketleri elde etmesinin önüne geçebilmektedir. UNIX sistemlerinde ifconfig komutunun çıktısında PROMISC bayrağı bulunuyorsa sistemde koklama yapılıyor demektir [54].

3.32. Kandırıcı (Spoofer)

Kandırıcılar, saldırganın IP adreslerinin sahtelerini üretmek (IP kandırma, IP spoofing) amacıyla kullanılır. Şirinler (Smurf, çizgi film) ve Fraggle (Muppet şov'daki yaratıklara verilen ad) saldırıları, bugünlerde kullanılan kandırma saldırılarının en başında gelenleridir. Saldırılmak istenen hedef makinenin adresi, paketi gönderen adres olarak yazıldığı bir 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 kandırıcı dışında, başka isimle e-posta mesajı göndermeye yarayan e-posta kandırıcı ve bir web sitesinin sahtesinin yayınlanmasıyla yapılan web kandırıcı yöntemleri de bulunmaktadır [20].

3.33. Casus Yazılım Çerezleri (Spyware Cookie)

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.

3.34. İz Sürme Çerezleri (Tracking Cookie)

Bir kullanıcının İnternet üzerinde gezinme geçmişini izlemek amacıyla, iki veya daha fazla web sayfasında paylaşılan çerezler iz sürme çerezleri olarak adlandırılmaktadır [55].

3.35. Turta (PIE)

PIE (Persistent Identification Element, İnatçı Kimlik Elemanı) olarak adlandırılan yapılar, birçok tarayıcı ve karşı casus yazılımların iz sürme çerezlerini engellemeleri sonucunda ortaya çıkan arayışın son örneklerinden biridir. Hali hazırda kullanılan 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 Macromedia Flash Player, Mart 2005'e göre % 98 ile birinci sırada bulunmaktadır [56]. 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.

3.36. Damlatıcı (Trickler)

Otomatik yazılım indirme tekniklerini kullanan bu casus yazılım, arka planda gizli ve çok yavaş bir şekilde (damla damla) bir yazılımın, hedef bilgisayara indirilmesini ve indirilen bu yazılımın kullanıcının haberi olmadan kurulmasını sağlar. Damlatıcılar, bir casus yazılımın bilgisayara sessizce kurulumuna olanak sağladığı gibi; kullanıcı o casus yazılıma ait bazı bileşenleri, karşı casus yazılımlar kullanarak veya bizzat silerek kaldırdığında, eksik öğeleri tekrar indirerek casus yazılımın bilgisayar kayıtlarının sürdürmesine de yol açması açısından tehlikeli yapılardır.

3.37. Savaş Telefon Çeviricileri (War Dialer)

Hayalet program telefon çevirme (demon-dialing) ve taşıyıcı tarama (carrier-scanning) olarak da adlandırılan savaş telefon çeviricileri, 1983'de yapılan "Savaş Oyunları" (War Games) filmi ile popülerlik kazanmıştır [57]. Bu türde bir aralıktaki telefon numaraları çevrilir ve çağrıyı otomatik olarak cevaplayan bir makine aranır. Birçok kuruluşun bu tür çağrıları cevaplaması için kullandığı modem takılı makineleri bulunmaktadır. Bu makinelere yapılacak saldırılar bu araçlarla saptanmaktadır [18].

3.38. Tavşanlar (Wabbit)

Virüs ve solucanlar dışında daha az yaygın olan "tavşanlar", kendi kendine çoğalan diğer bir tür kötücül yazılım türüdür [58]. Virüsler gibi konak program veya belgelerine bulaşmazlar ve solucanlar gibi diğer bilgisayarlara yayılmak için ağ yeteneklerini kullanmazlar. UNIX komutu "fork" ile çok miktarda proses üreten "fork bombası" en basit wabbit örneğidir [59].

İngilizce önerilen isim, "Buggs Bunny" çizgi filminde, Elmur Fudd adındaki tavşanı avlamaya çalışan çizgi roman kahramanının, tavşanı (rabbit) söyleme şeklinden gelmektedir. Doğada bulunan tavşanlar gibi, bu kötücül yazılımlar da hızlı bir şekilde çoğalma yeteneğine sahiptir.

4. SONUÇLAR VE DEĞERLENDİRMELER (RESULTS and CONCLUSIONS)

Bu çalışmada, bilgi ve bilgisayar güvenliğini tehlikeye sokan kötücül ve casus yazılımlar kapsamlı olarak araştırılmış, incelenmiş, sınıflandırılmış ve karşılaşılabilecek tehlikeler göz önüne serilmiştir.

Literatür incelendiğinde, kötücül ve casus yazılımlar üzerine böyle kapsamlı bir çalışmanın ilk kez yapılmış olması, magazinsel ve ticari bilgilerin dışında bu konunun akademik gündeme taşınması açısından da önem arz etmektedir.

Bilgisayar kullanıcılarının karşılaşabilecekleri tehlike ve tehdidin boyutlarını ayrıntılı bir biçimde sunmak, bu çalışmanın diğer bir önemli katkısı olarak değerlendirilmektedir.

İnceleme sonucunda; bilginin ve teknolojinin iç içe olduğu, baş döndürücü bir hızda gelişen elektronik ortamlarda, her zaman yanı başımızda olacak bilişim korsanları gibi kötü niyetli kişilerin ve sistemlerin açığını bulma da, bu açıkları kullanıp sistemlere izinsiz erişmede, sistemlere ve sistemi kullanan kişilere, kişisel veya kurumsal zarar vermede hemen hemen her yolu denemeye çalıştıkları tespit edilmiştir. Bu saldırılara ve tehditlere karşı tedbir alınabilmesi için, bu tür yazılımların ve kullandıkları yöntemlerin sürekli olarak incelenmesi gerektiği, elde edilen bulgular arasındadır.

Dünyada ve ülkemizde kötücül ve casus yazılımların yaygın olarak kullanımda olduğu; fakat kullanıcıların bu tehlike ve tehditlerinden çoğunlukla haberdar olmadığı anlaşılmıştır. Kişisel veya kuramsal her hangi bir zararla karşılaşılmaması için, konuya gereken önemin verilmesi, bilgi birikiminin arttırılması, hassasiyet gösterilmesi ve gereken önlemlerin alınması gerekmektedir.

Bu çalışmada, sahip oldukları karakteristiklerinin, kullanım amaçlarının, var olan çeşitlerinin ve kullandıkları yöntemlerin özetlendiği en genel kötücül yazılımlar arasında yer alan; virüsler, solucanlar, Truva atları, arka kapılar, mesaj sağanakları, kök kullanıcı takımları, telefon çeviriciler, korunmasızlık sömürücüleri, klavye dinleme sistemleri, tarayıcı soyma ve casus yazılımlar ile beraber bir araya getirilerek sunulan, çoğu yeni, 38 kötücül yazılım genel olarak değerlendirildiğinde;

- Ana ve yaygın bir şekilde bilinen kötücül yazılımların dışında; reklâm, parazit, hırsız, püsküllü bela yazılım, tarayıcı yardımcı nesnesi, uzaktan yönetim aracı, ticari RAT, bot ağı, ağ taşkını, saldırgan ActiveX, Java ve betik, IRC ele geçirme savaşı, nuker, paketleyici, ciltçi, şifre yakalayıcılar - soyguncular, şifre kırıcılar, anahtar üreticiler, e-posta bombardımanı, kitle postacısı, adres hasatçı, web böcekleri, aldatmaca, sazan avlama, web sahtekârlığı - dolandırıcılığı, telefon kırma, port tarayıcılar, sondaj aracı, arama motoru soyguncusu, koklayıcı, kandırıcı, casus yazılım ve iz sürme çerezleri, turta, damlatıcı, savaş telefon çeviricileri ve tavşanlar adı altında ve her biri farklı amaçlara yönelik değişik yöntemler kullanan çok çeşitli kötücül yazılımın var olduğu,
- Teknolojik olarak korunma teknikleri artarken tehditlerde de artış olduğu,
- Kötücül yazılımların teknolojik yenilikleri sıkı bir şekilde takip ederek hızla şekil değiştirdiği,
- Çoğunlukla, insanların bilgisizliklerinden, tecrübesizliklerinden ve zaaflarından faydalanıldığı,
- Kullanıcıların akıllarına bile gelmeyecek birçok masumane yaklaşımların kullanıldığı,
- Bilgisayar teknolojilerinde var olan açıklardan faydalanmanın yanında genelde göz ardı edilen sosyal mühendislik yaklaşımlarına da çok sık başvurulduğu,
- Web teknolojilerinin, bu yazılımların çok kısa sürede ve kolayca yayılmasına ve yaygınlaşmasına olanak verdiği,
- Bir sistemin ne kadar karmaşık ya da ne kadar fazla özelliğe sahipse, o kadar hata kipine ve güvenlik zayıflığına sahip olacağı,
- Kullanıcıların bilgisayar kullanma alışkanlıklarından, İnternet gezinme geçmişini incelemeye, mevcut port açıklarını tespit etmeye, işletim sistemi ve program korunmasızlık açıklarından yararlanmaya, önemli kritik ve kişisel bilgileri kötü niyetli kişilere göndermeye, bilgisayar sisteminde fark edilmeden ve iz bırakmadan çalışmaya, kullanıcı bilgisizlik ve zaaflarından faydalanmaya, kullanılan şifrelerin kırılmasına ve yakalanmasına, kendilerini farklı yazılımlar içerisinde saklayarak kötücül ve casus yazılım tarayıcıları ve koruma programlarını atlatmaya, hatta bu yazılımları devre dışı bırakmaya, bant genişliği, işlemci gibi sistem kaynaklarını fark ettirmeden dışarının kullanımına açmaya kadar birçok yöntem kullandıkları,
- Bilgisayar sistemlerine çeşitli yollarla kurulan, sisteme gizlice yerleşen, varlığını kullanıcıya fark ettirmeden çalışan ve sistem hakkında her türlü bilgiyi saldırganlara hızlıca aktaran (mesela e-posta kullanarak) casus yazılımların, kişisel gizliliği çiğneyerek kimlik hırsızlığına neden oldukları,
- Bilgi ve bilgisayar güvenliği konusunda güvenilir sistemler oluşturmak için bu tür yazılımların sürekli olarak takip edilmesi ve gerekli tedbirlerin kısa sürede alınması gerekliliği

tespit edilmiştir.

Kötücül yazılımların geleceği genel olarak değerlendirildiğinde aşağıdaki konular ön plana çıkmaktadır:

- Kötücül yazılımların önemli bir süre önemli bir güvenlik konusu olarak kalacağı düşünülmektedir. Sonuç

olarak, kötücül yazılım üreticileri, bilgisayar kullanıcılarından her zaman iki adım önde olacaktır [43].

- Sistemlere zarar vermekten çok, sistemleri her zaman potansiyel kullanımlar için elde tutacak ve kullanıcıları kuşkulandırmayacak, arka kapı ve uzaktan erişim araçları gibi kötücül yazılımlar ağırlık kazanacaktır [60].
- Farklı kötücül yazılım karakteristiklerinin bir araya getirilerek harmanlanmasından oluşan bileşim kötücül yazılımlar (combo/combination malware) da artış yaşanabilecektir. Bu tür kötücül yazılımlar daha hızlı yayılabilecek ve daha fazla zarara yol açabilecektir [61].
- Code Red ile beraber, 4. kuşak kötücül yazılımların ilgi alanı diz üstü bilgisayarlara doğru kaymaktadır. İleride kötücül yazılımların diz üstü bilgisayarların güvenlik açıklarını hedef alacak çok yönlü uygulamaları görülebilecektir [2]. Birçok işyeri için diz üstü bilgisayarlar, çözülmeyi bekleyen önemli bir kötücül yazılım sorunudur.
- Mesaj sağanakları (spam), bir süre daha para kazanmak isteyen bilgisayar meraklılarının ilgisini çekecektir.
- Mali kazanç olanaklarının arttığı ve teknik imkânların geliştiği bir ortamda, daha da az bilgi ve tecrübeye ihtiyaç duyacak kötücül yazılım yazarlarının artacağı düşünülmektedir. Dolayısıyla, kötücül yazılımlar gerek miktar gerekse kapsam bakımından daha da artmaktadır.
- Kendi kendini kontrol eden, kendini yeniden oluşturan ve kötücül yazılım tarayıcılarına karşı aktif savunma yapan, daha müzmin kötücül yazılım türlerinin ortaya çıkacağı ön görülmektedir [62].
- Kötücül yazılımlara karşı, saptamadan çok önleme konusuna ağırlık veren bir savunma anlayışının etkin bir şekilde geliştirilmesi ve sürdürülmesi gerekmektedir. Saptama konusunda da sezgisel yaklaşımlar geliştirilmelidir.

Bu inceleme çalışmasının amacı, her ne kadar en tehlikeli sanal dünya tehditlerinden olan kötücül ve casus yazılımların bir arada gözden geçirilmesi olsa da; bu tehditlere yönelik korunma yaklaşımları da gözden geçirilmiştir [1,5–7,9,29,37,43,45,63]. Bu çerçevede; kötücül ve casus yazılımlarla ilgili karşılaşılabilecek tehdit, tehlike ve riski en aza indirgemek için;

- Konu hakkında bilgi birikimi ve deneyimlerin artırılması,
- İşletim sistemi ve programlara ait güvenlik ve sistem güncellemeleri ve yamalarının düzenli bir şekilde yapılması ve bu yapıların en güncel olanlarının kullanılması,
- Korunma yaklaşımlarının belirlenmesi ve uygulanması,
- Güvenlik politikaları geliştirerek bunların uygulanmasının sağlanması ve takibinin yapılması,
- Bu politikaların yeni koşul ve uygulama sonuçlarına göre sürekli gözden geçirilip iyileştirilmesi ve geliştirilmesi,
- Bu politikalar arasında kullanıcı parolalarının oluşturulma kurallarının belirlenmesi ve uygulanması,
- Parolaların düzenli bir şekilde değiştirilmesinin sağlanması,
- Kullanıcı haklarının asgari seviyede tutulması,
- Sistemlerde ihtiyaç duyulmayan servis ve programların kapatılması veya kaldırılması gibi hayat kurtaran yaklaşımların kullanılması,
- Bilgi ve bilgisayar güvenliğinin sadece yazılım ve donanım ile sağlanamayacağının farkında olunması,
- İnsan faktörünün devreye girdiği sosyal mühendisliğin hiç bir şekilde göz ardı edilmemesi,
- Kişisel olduğu kadar kurumsal yaklaşımların da dikkate alınması,
- Bilgi ve bilgisayar güvenliği konusunda, işyerlerinde etkin bir şekilde görev alacak profesyonellerin yetiştirilmesi ve istihdam edilmesi,
- Mevcut personelin eğitilmesi,
- Kötücül yazılım korunma ve tarama programlarının geliştirilmesi ve kullanıcılar tarafından düzenli ve en güncel hali ile kullanılması,
- Mutlak surette, güncel virüs korunma programlarının kullanılması,
- Güvenlik duvarları ile sistem güvenliğinin sıkılaştırılması,
- Saldırı tespit sistemleri kullanılması,
- Mesaj sağanağı (spam) temizleyici veya uyarıcı yazılımların kullanılması,

gerekmektedir.

Bunun yanında, ülkemize özel olarak; bu tür konuların magazinden ziyade akademik çevrelerde de konuşuyor, tartışılıyor ve üzerinde çalışılıyor olması gereklidir. Bunun için;

- Konuyla ilgili olarak ülkemizde gündem oluşturulması,
- Üniversitelerimizde konu ile ilgili araştırmaların yapılması,
- Lisans seviyelerinde bilgi ve bilgisayar güvenliği derslerinin açılması,
- Bilgi güvenliği konularına üniversite öğrencilerin ilgisinin arttırılması, ya da en azından enformatik derslerinde mutlaka konunun ele alınması,
- Lisansüstü seviyede konuyla ilgili dersler açılması, araştırma ödevleri ve uygulamalar geliştirilmesi,
- Ürün ve çözümler üretecek bilgi ve bilgisayar güvenlik firmalarının, yeni güvenlik yazılımları geliştirmelerine özel teşvikler verilmesi

gerekmektedir.

Bilgisayar, internet ve bilgisayar ağlarının her geçen gün arttığı ve hayatımızı gün geçtikçe daha da fazla etkileyen, değiştiren ve yönlendiren sanal dünyanın getirilerinin, faydalarının, kazanımlarının ve olumlu yönlerinin yanında; eğer dikkat edilmez ise, kişisel ve kurumsal işleyişi sekteye uğratacağı, verimliliği düşüreceği, büyük boyutlarda zararlara yol açacağı,

hatta çok ciddi yerel veya küresel bir kargaşaya neden olabileceği değerlendirilmektedir.

Sonuç olarak her bilgisayar kullanıcısının;

- İster işyerinde ve/veya evinde, isterse internet kafelerde olsun, sanal dünyanın tehditlerinin her zaman farkında olması,
- Konu ile ilgili bilgi birikimini arttırması,
- Gündemi takip edip bilgilerini güncellemesi,

Kullanmış olduğu güvenlik sistem ve yazılımlarını düzenli olarak güncellemesi,

- Güvenlik politikaları oluşturup uygulanması,
- Her zaman uyanık olması ve olumsuz veya istenilmeyen bir durumla karşılaşınca alabileceği karşı tedbirleri önceden belirlemesi ve
- Güvenlik yaşam döngüsünün uygulanması,

gerekmektedir.

Aynı zamanda, bu çalışmanın, kötücül ve casus yazılımlar hakkında ciddi bilgi eksikliğini gidereceği, akademik camiada gündem oluşturacağı, ileride bu konuda yapılacak çalışmalara da ışık tutacağı değerlendirilmektedir.

TEŞEKKÜR (ACKNOWLEGEMENT)

Bu çalışma, Gazi Üniversitesi BAP tarafından desteklenen "**Bilgi ve Bilgisayar Güvenliği İçin Zeki Yazılımlar Geliştirme"** 06/2005–44 no'lu Gazi Üniversitesi Bilimsel Araştırma Projeleri kapsamında yapılmıştır. Yazarlar, Gazi Üniversitesi BAP Başkanlığı'na teşekkür eder.

KAYNAKLAR (REFERENCES)

1. Canbek, G., **Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme**, Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, 13, 31-32, 43, 50, 58, 154, Eylül 2005.
2. Heiser, J. G., **Understanding Today's Malware**, Information Security Technical Report. Vol. 9, No. 2, 47-64, April-June 2004.
3. Calder, A., Watkins, S., **It Governance: A Manager's Guide to Data Security & BS 7799/ISO 17799**, Kogan Page, 14, 163, September 1, 2003.
4. Thompson, R., **The Four Ages of Malware**, Infosecurity Today, 47-48, March/April, 2005.
5. Grimes, R. A., **Malicious Mobile Code**, O'Reilly, 3, 201-203, 226-228, 238-244, 467-468, August 1, 2001.
6. İnternet: **How Bad Is The Malware Problem?**, http://searchsmb.techtarget.com/sDefinition/0,sid44_gci991471,00.html, Eylül 2005.
7. İnternet: **2005 CSI/FBI Computer Crime and Security Survey**, http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml , Computer Security Institute, Kasım 2005.
8. İnternet: **Spyware and Increasing Security Risks-Proactive Protection for fhe Enterprise Client**, http://enterprisesecurity.symantec.com/content/webcastinfo.cfm?webcastid=146, Kasım 2005.
9. İnternet: Symantec, **Symantec Internet Security Threat Report, 2005**, http://ses.symantec.com/WP000ITR8, Kasım 2005.
10. Peikari, C., Fogie, S., **Maximum Wireless Security**, Sams Publishing, 153, 164, December 18, 2002.
11. Skoudis, E., **Malware: Fighting Malicious Code**, Prentice Hall PTR, 13, 96, 123-125, 149-151, 179, November 7, 2003.
12. İnternet: Symantec Security Response - W95.CIH, http://www.symantec.com/avcenter/venc/data/cih.html , Ekim 2005.
13. Mohay, G., Collie, B., Vel, O., McKemmish, R., Anderson, A., **Computer and Intrusion Forensics**, Artech House, 236, April 1, 2003.
14. Gustin, J., **Cyber Terrorism**, Marcel Dekker, 26-27, October 15, 2003.
15. Russell, D., Gangemi, Sr. G.T., **Computer Security Basics**, O'Reilly, 82, July 1, 1991.
16. Thompson, D. P., **The Trojan War: Literature and Legends from the Bronze Age to the Present**, McFarland & Company, 33, January 6, 2004.
17. İnternet: Trojan Programs, VirusList, http://www.viruslist.com/en/virusesdescribed?chapter=152540521 , Eylül 2005.
18. Hansen, J. B., Young, S., **The Hacker's Handbook**, CRC Press, 72-74, 126, 530, 714, November 24, 2003.
19. Conway, R., Cordingley, J., **Code Hacking: A Developer's Guide to Network Security**, Charles River Media, 55-56, 92, May 1, 2004.
20. Cole, E., **Hackers Beware: The Ultimate Guide to Network Security**, Sams Publishing, 104-108, 191-193, 544, 550, August 13, 2001.
21. Hansche, S., Berti, J., Hare, C., **Official (Isc) 2 Guide to the Cissp Exam**, CRC Press, 590, December 15, 2003.
22. Connally, K. I., **Law of Internet Security and Privacy 2004**, Aspen Publishers, Inc., 112, 2004.
23. İnternet: **Email Spam Statistics and Information**, McAfee, http://us.mcafee.com/fightspam/default.asp?id=stats , Eylül 2005.
24. **May 2005 Symantec™ Spam Statistics**, http://www.symantec.com/region/reg_ap/promo/brightmail/docs/May2005SpamStats.pdf, Eylül 2005.
25. Mohay, G., Collie, B., Vel, O., McKemmish, R., Anderson, A., **Computer and Intrusion Forensics**, Artech House, 226, April 1, 2003.
26. Caloyannides, M. A., **Privacy Protection and Computer Forensics**, Artech House, 118-120, October 1, 2004.

27. Gralla, P., Schaeffer, J. P., **The Complete Idiot's Guide to Internet Privacy and Security**, Alpha Books, 37, January 4, 2002.
28. Bishop, M. A., **Computer Security: Art and Science**, Addison-Wesley Professional, 724-725, December 2, 2002.
29. Tipton, H. F., Krause, M., **Information Security Management Handbook**, CRC Press, 132, 1254-1255, December 30, 2003.
30. Russell, R., **Hack Proofing Your Network**, Syngress Publishing, 78, January 1, 2001.
31. İnternet: Gostev A., **Malware Evolution: January - March 2005**, Kaspersky Lab. http://www.viruslist.com/en/analysis?pubid=162454316 , Nisan 2005.
32. Reynolds, J., **Complete E-Commerce Book: Design, Build and Maintain a Successful Web-Based Business**, CMP Books, 365, April 1, 2004.
33. Stephenson, P., **Investigating Computer-Related Crime**, CRC Press, 57-58, September 28, 1999.
34. Mutton, P., **IRC Hacks**, O'Reilly, 39-41, July 27, 2004.
35. Hausman, K. K., Barrett, D., Weiss, M., **Exam Cram 2 Security +: Exam Cram SYO-101**, Que Publishing, 59, April 10, 2003.
36. Mandia, K., Prosise, C., **Incident Response Second Edition: Computer Forensics**, McGraw-Hill Professional, 389-390, July 17, 2003.
37. İnternet: **Binder**, SearchWin2000, TechTarget. http://searchwin2000.techtarget.com/sDefinition/0,,sid1_gci948478,00.html , Mayıs 2005.
38. Poole, O., **Network Security: A Practical Guide**, Elsevier, 69-71, December 9, 2002.
39. Pipkin, D. L., **Halting the Hacker - A Practical Guide to Computer Security**, Prentice Hall PTR, 52, August 26, 2002.
40. Bace, R. G., **Intrusion Detection**, Sams Publishing, 151, December 22, 1999.
41. İnternet : Zone Labs Virus Information Center, **Virus Glossary**, http://vic.zonelabs.com/tmpl/body/CA/virusGlossary.jsp , Ekim 2005.
42. Campbell, P., Calvert, B., Boswell, S., **Security+ in Depth**, Thomson Course Technology, 83, February 1, 2003.
43. Stewart, J., **This business of malware**, Information Security Technical Report. Vol. 9, No. 2, 35-41, April 2004.
44. Mena, J., **Homeland Security Techniques and Technologies**, Charles River Media, 47-48, May 10, 2004.
45. Vacca, J. R., **Computer Forensics - Computer Crime Scene Investigation**, Charles River Media, 489-490, May 1, 2005.
46. Burgess, R. C., Small, M. P., **Computer Security in the Workplace**, SEO Press, 21, 2005.
47. Shimonski, R. J., Johnson, N. L., Crump, R. J., **Security+**, Syngress Publishing, 142-143, December 1, 2002.
48. Bennett, J., **Digital Umbrella: Technology's Attack on Personal Privacy in America**, Brown Walker Press (FL), 47-50, September 1, 2004.
49. Gralla, P., **Windows XP Hacks**, O'Reilly, 152-157, April 1, 2005.
50. İnternet: **Sanal Dolandırıcılıkta Son Nokta Phishing**, İstanbul Emniyet Müdürlüğü. http://www.iem.gov.tr/iem/?idno=147, Mayıs 2005.
51. İnternet: **Consumer Online: Home > Scams > Major Scams**, http://www.consumer.org.nz/topic.asp?docid=253&category=&subcategory=&topic=Scams&title=Major%20Scams&contenttype=summary , Eylül 2005.
52. Brown, S., **The Complete Idiot's Guide to Private Investigating**, Alpha Books, 144-146, October 1, 2002.
53. Jones, S., **Encyclopedia of New Media: An Essential Reference to Communication and Technology**, Sage Publications Inc, 212-216, December 10, 2002.
54. Orebaugh, A. D., **Ethereal Packet Sniffing**, Syngress Publishing, 6-10, 27-28, February 17, 2004.
55. Garfinkel, S., **Web Security, Privacy & Commerce**, 2nd Edition, O'Reilly, 216-221, November 1, 2001.
56. İnternet: **Macromedia Flash content reaches 98.3% of Internet viewers**, Flash Player Penetration Survey, March 2005, NPD Research. http://www.macromedia.com/software/player_census/flashplayer/ , Haziran 2005.
57. Petersen, J. K., **Understanding Surveillance Technologies**, CRC Press, 2-9, September 21, 2000.
58. İnternet: **Self Replicating Wabbits – Sounds Strange. Brings Chaos**, SYL Articles, http://articles.syl.com/selfreplicatingwabbitssoundsstrangebringschaos.html, Eylül 2005.
59. Chuvakin, A., Peikari, C., **Security Warrior**, O'Reilly, 324, January 12, 2004.
60. Furnell, S., Ward, J., **Malware comes of age: The arrival of the true computer parasite**, Network Security, 11-15, October 2004.
61. Williamson, D., **Deconstructing malware: what it is and how to stop it**, Information Security Technical Report. Vol. 9, No. 2, 27-34, 2004.
62. Levenhagen, R., **Trends, codes and virus attacks - 2003 year in review**, Network Security, Vol. 2004, No. 1, 13-15, January 2004.
63. **Hacker 2004 Raporu**, Chip Dergisi, Nisan 2004, 44-61, 2004.