T.C.
FIRAT ÜNİVERSİTESİ
TEKNOLOJİ FAKÜLTESİ

Casus ve Zararlı Yazılımların İncelenmesi

Serdar ARIKAN

YMH455 Bitirme Projesi

Yazılım Mühendisliği Bölümü

Haziran 2022

T.C.
FIRAT ÜNİVERSİTESİ
TEKNOLOJİ FAKÜLTESİ

Yazılım Mühendisliği Bölümü

YMH455 Bitirme Projesi

Casus ve Zararlı Yazılımların İncelenmesi

Tez Yazarı

Serdar ARIKAN

Danışman

Prof. Dr. Resul DAŞ

Haziran 2022
ELAZIĞ

Beyan

Fırat Üniversitesi Teknoloji Fakültesi tez yazım kurallarına uygun olarak hazırladığım "Casus ve Zararlı Yazılımların İncelenmesi" başlıklı YMH455 Bitirme Projesimin içindeki bütün bilgilerin doğru olduğunu, bilgilerin üretilmesi ve sunulmasında bilimsel etik kurallarına uygun davrandığımı, kullandığım bütün kaynakları atıf yaparak belirttiğimi, maddi ve manevi desteği olan tüm kurum/kuruluş ve kişileri belirttiğimi, burada sunduğum veri ve bilgileri unvan almak amacıyla daha önce hiçbir şekilde kullanmadığımı beyan ederim.

11/06/2022

Serdar ARIKAN

İçindekiler

Sayfa

Özet

Casus ve Zararlı Yazılımların İncelenmesi

Serdar ARIKAN

YMH455 Bitirme Projesi

Fırat Üniversitesi
Teknoloji Fakültesi

Yazılım Mühendisliği Bölümü
Haziran 2022

Bilgisayarların daha azla kullanıcı tarafından kullanılmaya başlanması ile başlayan kişisel veri kavramı ve bu kişisel verilerin korunması gerekliliğine olan ihtiyaç giderek artmaktadır. Bilgisayar korsanları sürekli kendilerini geliştirerek sürekli yeni casus ve zararlı yazılımlar üretmektedirler. Bu çalışmada bilgi güvenliğinin ne olduğu ve tarhiçesinin ne olduğunun incelenmesiyle başlanmıştır. Daha sonra literatürde bulunan çalışmalar analiz edilmiş ve ardından casus ve zararlı yazılımların bulaşma teknikleri, belirtileri ve türleri incelenmiş ve son olarak bu tür yazılımlara karşı alınması gereken önlemlerin açıklanmasıyla çalışma tamamlanmıştır. Bu çalışma sonucunda kullanıcıların casus ve zararlı yazılımlara karşı daha bilinçli savunma yapmaları hedeflenmektedir.

Anahtar Kelimeler: Casus yazılım, zararlı yazılım, antivirüs, anticasus,bilgi, bilgi güvenliği, kişisel veri..

Abstract

Investigation of Spyware and Malware

Serdar ARIKAN

YMH455 Bitirme Projesi

Firat University
Faculty of Technology

Department of Software Engineering
June 2022

The concept of personal data, which started with the use of computers by fewer users, and the need for the protection of this personal data are gradually increasing. Hackers are constantly improving themselves and constantly producing new spyware and malware. This study started by examining what information security is and what its history is. Afterwards, the studies in the literature were analyzed and then the infection techniques, symptoms and types of spyware and malware were examined, and finally the study was completed by explaining the precautions to be taken against such software. As a result of this study, it is aimed that users can defend themselves more consciously against spyware and malware.

Keywords: Spyware, malware, antivirus, antispy, information, information security, personal data..

Şekiller Listesi

Sayfa

Tablolar Listesi

Sayfa

1. Giriş

Siber güvenlik yada bilgi güvenliği kişisel bilgisayarların çıkışından beri kullanıcılar için önemli kavramlar olmuşlardır. Kişisel bilgisayar kullanıcıları daha önceki kullanıcılar olan bilim insanları kadar bilinçli kullanıcılar değillerdi. Bunu fırsat bilen kötü amaçlı kişiler kişisel bilgisayarlara sızarak içerisindeki önemli bilgileri çalmak için harekete geçtiler. Bu kişiler hacker veya bilgisayar korsanları olarak adlandırılırlar. Zaman içerisinde yeni yöntemler geliştiren bilgisayar korsanları daha karmaşık ve daha fazla zarar verici saldırılar yapmaya başlamışlardır. Onlara karşı durabilmek için bazı şirketler antivirüs denilen ve bu zararlı yazılımları tespit edip etkisizleştirebilen yazılımlar geliştirmişlerdir.

Bilgisayar bilimlerinde veri (data), işlenmeye hazır ham bilgi olarak ifade edilir. Etimolojik olarak Latince datum kelimesinin çoğuludur [9]. Veriler tamsayı, karakter veya sembollerden oluşabilir. Bu veriler türlerine göre veri yapısı denilen ortamlarda saklanırlar. Veriler saklama birimlerinde binary (0 ve 1) dizileri şeklinde tutulur. Aynı bit dizisi veri türüne göre farklı içerikte olabilirler. Örneğin '01010110' dizisi tamsayı veri türünde '86' değerini taşırken karakter veri tipinde 'V' harfine denk gelmektedir.

Kişisel veri, bir kişinin kimliğini belirten veya belirtebilecek veriler için kullanılmaktadır. Bu veriler ad, soyad, adres gibi genel bilgiler olabileceği gibi parmak izi vb. biyolojik bilgiler de olabilir. Aynı şekilde kişinin kullandığı elektronik ortamlardaki IP adresi, e-mail adresi de kişisel veriler kapsamına girmektedir. Bu tip verileri korumak için devletlerin kendi hukuk sistemlerinde çeşitli yasalar mevcuttur. Ancak bu yasalar haricinde bilgisayar bilimcileri de kişisel verileri korumak amacıyla çeşitli uygulamalar geliştirmişlerdir. Bu tür hizmetler bilgi güvenliği olarak adlandırılır.

Bu çalışmanın öncelikli amacı kullanıcıları bilgisayar korsanlığına karşı bilinçlendirmek ve daha iyi korunmaları için yardımcı olmaktır. Çalışmanın içeriğinde bilgi güvenliğinin tarihsel gelişiminden kişisel veerilerin önemine, casus ve zararlı yazılımların bulaşma ve korunma yöntemlerinden türlerine ve önemli örenklerine kadar geniş bir içerik sunulmuştur. Aynı şekilde incelenen lieratür çalışmaları ile önemli ve faydalı kaynakların bir listesi sunulmuşur.

Bu bölümde veri kavramından ve kişisel verilerin korunmasından bahsedilmektedir. İkinci bölümde bilgi güvenliğinin ortaya çıkışı ve tarihsel gelişiminden bahsedilmektedir. Üçüncü bölümde konu hakkında literatürde bulunan çalışmaların incelenmesi yapılmaktadır. Dördüncü bölümde casus yazılımların, beşinci bölümde zararlı yazılımların özelliklerinden ve türlerinden bahsedilmektedir. Altıncı bölümde casus ve zararlı yazılımlardan korunma yöntemleri anlatılmaktadır.

2. Bilgi Güvenliği

Bilgi güvenliği, bilginin bir varlık olarak tehdit veya tehlikelerden korunması için doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak, bilginin varlığının her türlü ortam üzerinde istenmeyen kişiler tarafınca elde edilmesini önleme girişimi olarak tanımlanmaktadır.

Bilgi güvenliği; sağlanan servislerin, sistem ve verilerin korunmasını sağlar. Kullanıcılar bilgi güvenliğini kendi bakış açıları ile değerlendirdiğinde, basit bir tanım olarak; günlük hayatta kullanılan bilgisayar ve akıllı telefonlar ile sosyal medyaya girişin güvenliğinin sağlanması olarak düşünülebilir. Her kullanıcı özelinde bilişim sistemlerinin farklı imkanlar sunduğu düşünüldüğünde ve bunun sonucunda da bilgi güvenliği ifadesinin kişilere özgü olarak değişiklik göstereceği söylenebilmektedir.

Bilgi güvenliği, bilgiye karşı olan tehditlerle ilgilenmektedir. Bilgi güvenliğinin 'CIA' yani Gizlilik (Confidentiality), Bütünlük (Integrity) ve Kullanılabilirlik (Availability) olarak sağlamaya çalıştığı üç temel unsuru bulunmaktadır. [4]

Gizlilik (Confidentiality): Bilginin yetkisiz kişilerin eline geçmemesi, geçmesinin engellenmesidir.

Bütünlük (Integrity): Bilginin yetkisiz kişiler tarafından değiştirilmemesidir. Bilgi değiştirilebilir ancak yetkili olan kişiler tarafından ve ihtiyaca göre değiştirilmesi doğru olur.

Kullanılabilirlik (Availability): Bilginin ilgili ya da yetkili kişilerce ulaşılabilir ve kullanılabilir durumda olmasıdır. Bütünlük ve erişilebilirlik birbirlerine çok yakın ancak ters kavramlardır.

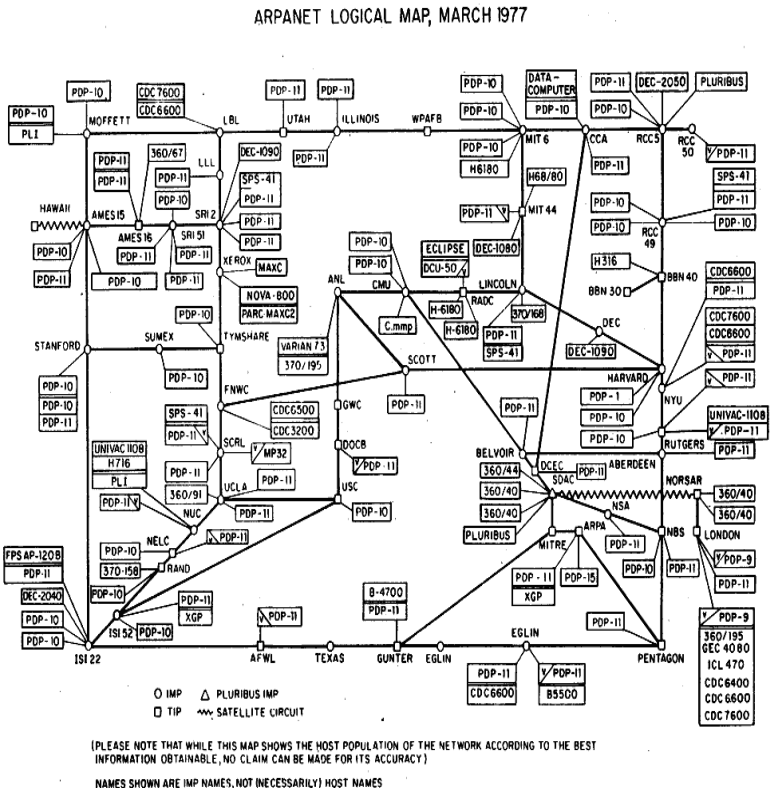
2.1. Bilgi Güvenliği'nin Tarihçesi

Bilgi Güvenliği'nin ilk örnekleri olarak tarihin eski devirlerinden beri süregelen askeri iletişim sırasında önemli bilgilerin düşman eline geçmesini engellemek amacıyla oluşturulmuş şifreleme tekniklerini gösterebiliriz. Bu tekniklere örnek olarak Roma Generali Julius Caeser'in geliştirmiş olduğu ve kendi adıyla anılan Sezar şifrelemesini verebiliriz. Bu yöntem ilgili metindeki karakterlerin alfabetik sıralamada 3 sıra sonraki harfle yer değiştirmesi ile oluşturulur. Modern zamandaki bilgi güvenliğinin gelişimi ise şu şekildedir;

1960'lar: Bu yıllarda bilgisayarlar bir odayı dolduracak büyüklükteydi. Bu bilgisayarlara erişim çok sınırlı olduğu için daha önce bilgi güvenliği ile ilgili endişe yaratacak bir durum yoktu. Ancak bu yıllardan itibaren bilgisayarlara erişimi olan bazı insanlar bazen meraktan bazen ise sistemlerin daha verimli çalışmasını sağlamak için ilk bilgisayar korsanlığı örneklerini gerçekleştirdiler.

1967'de IBM bir grup öğrenciyi yeni bilgisayarlarını denemeleri için davet etti. Öğrenciler denemeleri sonucu sistemin çeşitli alanlarına erişim sağladılar. Bu gelişmeden sonra sistemin güvenlik açıklarını gidermek bir amaç olarak ortaya çıktı. Bu olay ethical hacking'in ilk örneği olarak kabul edilebilir. Bu gelişmelerden sonra şirketler güvenliğe daha fazla yatırım yapmaya ve çeşitli önlemler almaya başladılar. Bilgisayarlara artık şifre konulmaya başlandı. Bunun bir sonucu olarak bilgisayarlar kilitli odalara konulmaktan vazgeçildi.

1970'ler: 1970'ler bigi güvenliğinin tam anlamıyla başladığı yıllar olarak kabul edilir. Bu yıllarda İleri Araştırma Projeleri Ajansı Ağı(ARPANET) projesi başladı. Bu proje daha sonra internetin öncülü bir hal almıştır. Şekil 2.1'de ARPANET ağının mantıksal haritası verilmiştir.



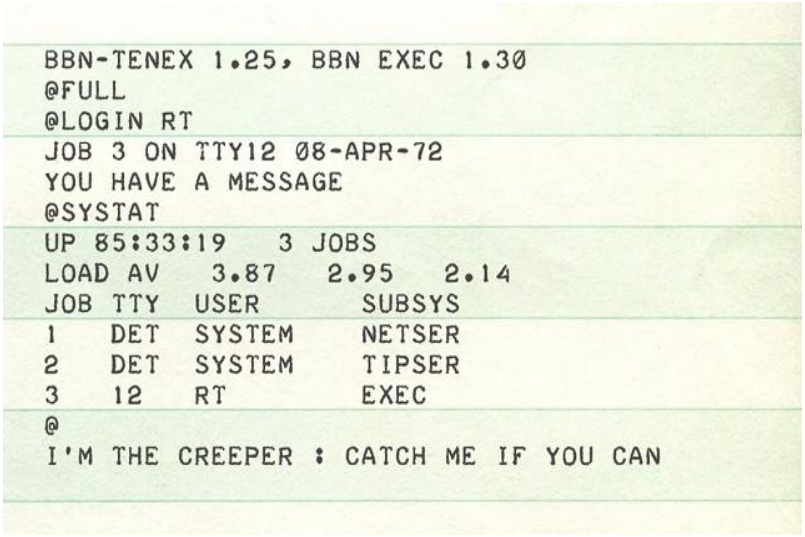
Şekil 2.1 ARPANETin mantıksal haritası [3]

Bob Thomas adında bir araştırmacı bu ağ içerisinde gezebilen ve arkasında bir mesaj bırakan bir program geliştirdi. "I'm the Creeper : Catch me if you can" mesajını bırakan bu programa mesajın içeriğinden dolayı "Creeper" adı verildi. Şekil 2.2'de Creeper programının arkasında bıraktığı çıktıyı görebilirsiniz.

Bu gelişmeden sonra e-postanın mucidi Ray Tomlinson Creeper'ı kovalayan bir başka program geliştirdi. Reaper adı verilen bu program aynı zamanda Creeper'ı siliyordu. Reeper virüsten korunma yazılımlarının ilki olmasının yanı sıra aynı zamanda kendi kendini kopyalayabiliyordu. Bu özelliği onu tarihteki ilk bilgisayar solucanı yaptı.

1980'ler: 1980'ler artık bilgisayar korsanlığının politik amaçlarla kullanılmaya başlandığı yıllar oldu. 1986 yılında Alman bir bilgisayar korsanı olan Marcus Hess ABD askeri sırlarını çalmak üzere PENTAGON'daki ana bilgisayarlar dahil toplam 400'den fazla bilgisayar sistemine girdi. Amacı bu bilgileri kopyalayıp Rusya'ya satmaktı ancak başarısız oldu.

Bu olaydan iki yıl sorna 1988'de Morris solucanı adı verilen bir bilgisayar solucanı geliştirildi. Bu solucanın öncelikli amacı bilgisayar sistemlerindeki açıkları tespit etmekti. Ancak solucan aşırı agresif bir şekilde çoğaldığı için hedef



Şekil 2.2 Creeper mesajı örneği [1]

bilgisayarları çalışamaz hale getirdi ve interneti yavaşlattı. Morris solucanının mucidi Robert Morris bu olaylar sonucunda Bilgisayar Sahtekarlığı ve Kötüye Kullanım Yasası uyarınca başarılı bir şekilde suçlanan ilk kişi oldu.

1989'da ARPANET ağı dünya çapında halka açıldı ve internete dönüşmeye başladı.

1990'lar: İnternetin halka açılmasıyla beraber birçok kişi kişisel bilgilerini çevrimiçi ortamlarda saklamaya başladı. Bunun bir sonucu olarak bilgisayar korsanları bu bilgileri çalmaya başladılar. Bu gelimelerin ardından Bir NASA araştırmacısı , binalarda gerçek yangınların yayılmasını önleyen fiziksel yapılar üzerinde modelleyerek ilk güvenlik duvarı (firewall) programını geliştirdi.

1999 yılında Melissa virüsü ortaya çıktı. E-posta üzerinden yayılan bu virüs ilk kullanıcının bilgisayarına bir Word belgesi üzerinden bulaştı. Ardından Microsoft Outlook üzerinden ilk 50 e-posta adresine kendi kopyalarını gönderdi. En hızlı yayılan virsüslerden biri olan Melissa virüsünün hasarı yaklaşık 80 milyon dolara mal oldu.

2000'ler: 2000'lerin başlarında hükümetler bilgisayar korsanlarına yönelik cezaları arttırdı. Artık 80'lerdeki gibi hafif cezalar yerine uzun süreli hapis ve büyük para cezaları verilmeye başlandı.

İnternet ağına daha fazla cihaz girmeye başlamasıyla beraber güvenlik açığı oluşturabilecek cihaz sayısı da artmış oldu. Bilgisayar korsanları bu cihazlara girebilmek için yeni bir bulaşma tekniği geliştirdi. Bu teknik kullanıcılar dosya indirmeden web üzerinden virüs bulaşmasını sağlıyordu. Temiz web sayfaları korsanlar tarafından virüslü sayfalarla değiştirdiğinden veya sayfalara kötü amaçlı yazılım sakladıklarından web sayfasını ziyaret etmek yeterli hale geldi.

2010'lar: 2010'lu yıllara geldiğimizde arık fidye yazılım türlerinin yoğun bir şekilde kullanılmaya başlandığını görüyoruz. 2000'li yılların ortalarında çıkmaya başlayan fidye yazılımlar 2010'lu yıllarda en revaçtta oldukları yılları yaşadılar. 2013

yılında Cryptolocker ve 2017 yılında Wannacry yazılımı büyük proramcılarına büyük kaançlar sağlamışır.

Cryptolocker yazılımı Microsoft Windows işletim sistemlerini hedef alır. CryptoLocker, virüslü e-posta eklerinden bilgisayara bulaşarak, bilgisayara bağlı depolama birimlerindeki ve bilgisayara bağlı ağlarda bulunan belirli türlerdeki dosyaları şifreler. Fidye olarak geleneksel para birimleri yerine Bitcoin ile ödeme yapılmasını istemektedir.

Wannacry mayıs 2017'de 99 ülkedeki 230.000 bilgisayara bulaşarak 28 dilde fidye talep eden geniş çaplı bir siber saldırı başlattı. Birçok hükümet kurumları ve önemli firmaların sistemlerine bulaşmıştır. 13 Mayıs 2017'de, Microsoft'un güncelleme desteği vermeyi çoktandır bıraktığı Windows XP, Windows 8 ve Windows Server 2003 için bir güvenlik güncelleştirmesi oluşturmak için olağan dışı bir adım attığı bildirildi. [24]

Gelecek: Kullanıcıların bilgisayarlar ve içerisindeki yazılımlar hakkında bilgileri artmaya başladıkça bilgisayar korsanları sistemlere sızabilmek için farklı yöntemler kullanmak zorunda kalmaya başladılar. Yeni silahları arasındaki en büyüğü ise sosyal mühendislik diye tabir ettiğimiz yöntemdir. Sosyal mühendislik insanlara farkettirmeden ilgilerini çekebilecek şşeyler kullanarak onları kandırmaya yarayan bir beceridir. Bilgisayar korsanları insanlara hediyeler, ücretsiz tatiller gibi cezbedici şeyler sunarak kötücül yazılımları farkettirmeden kurmayı başarıyor. Bilgisayar korsanlarının kullandığı bir başka yeni yöntem ise geleneksel para birimleri yerinr kripo para birimlerinin kullanımı. Kripto para birimlerinin hükümetler tarafından takip edilebilir olmamasından dolayı bunları kullanarak kendilerini gizlemeyi başarıyorlar.

3. Literatür İncelemesi ve Değerlendirilmesi

Casus ve zararlı yazılımlar Türkiye'de henüz gelişmekte olan bir alan olarak öne çıkmaktadır. Literatürde bulunan çalışmaları incelediğimiz zaman Şeref Sağıroğlu ve Gürol Canbek hocaların çalışmalarının öncü niteliğinde olduğunu görüyoruz. Birlikte yazdıkları [31] kitabı daha sonra gelen genç arkadaşlar için önemli bir kaynak olmuştur. Bu eserde bilgi güvenliği ve kriptoloji araştırmaları ile başlayan yazarlar daha sonra kötücül ve casus yazılımları tanımları, türleri ve güncel örnekleri ile incelemişlerdir. Kitabın sonlarında daha önce gerçekleştirilmiş önemli saldırılara yer veren yazarlar casus ve kötücül yazılımlardan korunma yöntemleri ile kitabı sonlandırmışlardır.

Literatürde bulunan çalışmalar genellikle casus ve kötücül yazılımların tanımını, belirtilerini, bulaşma tekniklerini ve korunma yöntemlerini incelemektedir. Bu çalışmalara örnek olarak [40], [36], [35], [32], [28], [33] verilebilir. Bir diğer önemli çalışma alanı ise teorik bilginin yanında bir uygulama ile örneklendiren çalışmalardır. [27], [30], [39] bu çalışmalara örnek olarak verilebilir. Tüm bu çalışmaları Tablo 3.1'nde bulabilirsiniz.

Tablo 3.1 Casus ve zararlı yazılımlar hakkında literatür incelemesi

Ref.	Yıl	Amaç Kapsam	Yöntem	Sonuç
[27]	2017	Android işletim sisteminde kötücül yazılımların tespit edilmesi.	İzin Tabanlı Analiz yöntemi kullanılarak KNN ve Naïve Bayes algoritmaları ile başarı oranı tespit edilmiştir.	Bu çalışma kapsamında geliştirilen sistem ile test verisinde bulunan kötücül yazılımların %97'den fazlası doğru bir şekilde tespit edilmiştir. Bu çalışma kapsamında, Android işletim sistemini kullanan mobil cihazlar için izin tabanlı bir kötücül yazılım tespit sistemi geliştirilmiştir.
[36]	2012	Üniversite öğrencilerinin antivirüs ve sahte antivirüsler hakkındaki bilgi seviyelerini ölçmek.	Anadolu Üniversitesi Bilgisayar ve Öğretim Teknolojileri Eğitimi bölümü ve Anadolu Üniversitesi 1,2,3 ve 4. Sınıf öğrencilerine virüsler ve sahte antivirüs programları ile ilgili anket uygulatılmıştır.	Ankete toplam 64 öğrenci katılmıştır. Anket sonucunda BÖTE öğrencilerinin %59'unun diğer bölüm öğrencilerinin ise %37'sinin sahte antivirüs programları hakkında bilgisi olduğu tespit edilmiştir. Ankete katılan tüm öğrencilerin virüsler hakkındaki bilgisi %75-%80 oran aralığındadır.
[35]	2012	Casus yazılımların sisteme bulaşma belirtilerinin ve önlemlerin açıklanması.	Casus yazılım bulaşma teknikleri açıklanmış ve daha sonra casus yazılımlar hakkında örnekler verilmiştir.	Casus yazılımların zararları ve neden önlenmesi gerektiği hakkında bilgiler verilmiştir. Kullanıcıların bilinçlenmesi amacıyla casus yazılımların belirtileri ve alınması gereken önlemler açıklanmıştır.
[32]	2007	Casus yazılımların belirtilerinin, bulaşma yöntemlerinin ve alınması gereken önlemlerin incelenmesi.	Belirtiler, bulaşma yöntemleri ve önlemler detaylandırılarak maddeler halinde ve örneklerle açıklanmıştır.	Kullanıcılara casus yazılımlar hakkında detaylı bilgiye sahip olmaları için gerekli örneklemeler ve açıklamalar yapılmış olup çalışmanın sonunda literatürde bulunan çalışmalardan da bahsedilerek ekstra kaynak önerisinde bulunulmuştur.
[40]	2007	Bilgisayar korsanları tarafından yapılan saldırı türlerinin incelenmesi.	Bilgisayar sistemlerine yapılan saldırılar grafik ve görsellerle desteklenerek ortaya konulmuştur.	Makale yazıldığı döneme ait istatistiki verileri barındırmaktadır. Bu istatistiklere göre bilgisayar korsanlarının saldırı yapmalarına en fazla sebep olan nedenler vatanperverlik, eğlence ve meydan okuma olarak tespit edilmiştir. Bir başka grafikte ise saldırı türlerinin giderek daha karmaşık yöntemlerle yapıldığı belirtilmiştir.

[28]	2018	Makale bir zararlı yazılım türü olan fidye yazılımları incelemeyi amaçlamaktadır.	Makalede daha önce yapılan fidye yazılım saldırılarının şirketleri uğrattığı kayıplardan bahsedilmektedir.	Makaleye göre 2017 yılında Barkly firması tarafından yayınlanan istatistiklere göre, şirketler ortalama 40 saniye de bir fidye yazılım saldırısına uğramakta ve her 10 zararlı yazılımdan 6 adedi fidye zararlısı olarak karşımıza çıkmaktadır. Ayrıca hedeflenen şirketlerin %71'ine fidye zararlısı bulaştırılmıştır. İstenen fidye tutarı yaklaşık olarak 1,077 dolara yükselmiştir. Saldırganlar tarafından talep edilen ödemeyi yapan beş şirketten birine dosyalarına erişim hakkı verilmemiştir. Bu şirketlerin %72'si sahip olduğu verilere ortalama 2 gün ve üzeri süreyle erişim sağlayamamıştır. Netice olarak küresel anlamda fidye yazılımların tahmini zararı 5 milyar dolar olacağı tahmin edilmektedir.
[30]	2007	Zararlı yazılımların farklı işletim sistemlerinde farklı tepkiler verip vermediği araştırılmıştır.	Farklı işletim sistemlerinde görülen zararlı yazılımlar incelenmiş ve zararları tespit edilmiştir.	Makalede yapılan araştırmalar sonucunda Java tabanlı olarak yazılan zararlı yazılımların tüm işletim sistemlerinde kullanıldığı görülmüştür. Bunun yanı sıra en çok Windows işletim sistemi saldırıya uğramaktadır, ikinci sırada Macintosh gelmektedir, en az saldırıya uğrayan ise Linux işletim sistemidir.
[39]	2019	Bu çalışmada sunulan, web tabanlı zararlı yazılımların saldırı ve analiz yöntemleri ve bunların uygulamasının kullanıcı farkındalığını arttıracağı, karşılaşılabilecek olumsuz örneklerin giderilmesine katkılar sağlayacağı değerlendirilmektedir.	Sırasıyla statik analiz, dinamik analiz ve kod analizi adımları uygulanmıştır.	Çalışmada ilk olarak kurban bilgisayarın yedeklemesini yapıp statik analiz kullanılarak şüphelenilen dosyalar analiz edilmiştir. Daha sonra zararlı yazılım olma ihtimali bulunan dosyalar www.virustotal.com web sitesi üzerinden taranmıştır. Sonrasında dinamik analiz aşamasına geçilmiştir. Tüm bu analizler sonucunda AutoKMS.exe, install.exe dosyalarının zararlı yazılım olduğu tespit edilmiştir.
[38]	2019	Bu çalışmada, Uzak Erişim Truva Atlarını (UETA) tanımlayarak, kurban sisteme sızma yöntemleri ve bu tehditte karşı alınabilecek önlemleri açıklayıp kullanıcı farkındalığı yaratması amaçlanmıştır.	Çalışmada UETA zararlı yazılımının bir örneği incelenmektedir.	Çalışma UETA yazılımlarının sızma yöntemlerinden ve daha sonrasında da alınabilecek önlemlerden bahsedilmesi ile başlıyor. Ardından örnek bir olayın incelenmesi ile devam edilmektedir. Kurban bilgisayarda son indirmeler incelenirken "NjRat 0.7d Golden Edition C432.zip" isimli şüpheli bir dosya bulunmuştur. Şüpheli dosya hakkında ilk önce statik analiz yapılmıştır. Statik analizde amaç şüpheli dosya çalıştırılmadan önceki yapısal analizini içermektedir. Statik analiz sayesinde şüpheli dosyanın içerdiği ve daha önce tespit edilmiş olabileceği için internet geçmişine ulaşılabilmektedir. "NjRat 0.7d Golden Edition C432.zip" isimli dosyanın, bünyesinde farklı antivirüs firmalarına ait tarama bilgileri barından "www.virustotal.com" web sayfası üzerinden online sorgulaması yapılmış olup söz konu dosyanın zararlı yazılım olduğu tespit edilmiştir.

4. Casus Yazilimlar

Casus yazılımlar (spyware) bir sisteme sızan ve kendini belli etmeden çalışan programlardır. Virüsler ve solucanlar gibi kendilerini kopyalama ihtiyaçları duymazlar. Casus yazılımların amacı donanıma zarar vermek değil bunun yerine bilgisayarınızda yaptığınız işlemleri ve bilgileri kopyalamaktır. Bu bilgiler tarayıcı geçmişiniz olabileceği gibi şifreleriniz, kredi kartı bilgileriniz, banka bilgileriniz, e-posta adresi ve telefon numaranız da olabilir. Elde edilen bu bilgiler genellikle bilgisayar korsanları tarafından satılmakta ve bu şekilde kar sağlanmaktadır. 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 [33].

"Casus yazılım" kelimesi ilk olarak Usenet'te 16 Ekim 1995'te Microsoft'un iş modeli hakkında mizahi bir yazıyla ortaya çıktı. Bir Lexis/Nexis araştırması, bu kelimenin, Zone Labs'ın Zone Alarm Personal Firewall için bir basın açıklamasında kullandığı 1999 yılına kadar küçük kameralar gibi casus ekipmanlar için kullanıldığını gösteriyor. Oradan, kelime hızla yaygın kullanıma girdi ve 2000'in başlarında ortaya çıkan ilk casus yazılım önleme programı Steve Gibson'ın OptOut'u ortaya çıktı [21]. PC Tools'un Casus Yazılım Doktoru, Lavasoft'un Ad-Aware SE ve Patrick Kolla'nın Spybot - Search & Destroy gibi programlar, casus yazılım programlarını kaldırmak ve bazı durumlarda engellemek için araçlar olarak hızla popülerlik kazandı. Aralık 2004'te Microsoft, GIANT AntiSpyware yazılımını satın alarak Microsoft AntiSpyware (Beta 1) olarak yeniden markalaştırdı ve Orijinal Windows XP ve Windows 2003 kullanıcıları için ücretsiz indirme olarak yayınladı. Kasım 2005'te Windows Defender olarak yeniden adlandırıldı [20].

Hemen hemen her yazılım, kurulumu esnasında kullanıcılara bir lisans anlaşması sunar ve kullanıcılar da genellikle bunu okumaya bile ihtiyaç duymadan onaylar. Çoğu zaman okunmayan bu lisans anlaşmalarının içeriğinde, internetten ücretsiz dağıtılan faydalı yazılımları kullanabilmek için kullanıcılar bilgisayarlarına casus yazılımların kurulmasını da kabul etmek zorunda bırakılır. "Freeware" ya da "Shareware" olarak bilinen ve genellikle web ortamından elde edilebilen bu yazılımların içerisinde gömülü olarak bulunan küçük yazılımlar kurulumla beraber kolayca bilgisayara yerleşebilirler [35].

4.1. Casus Yazılımlar Nasıl Çalışır

Yazılım tarafından kaydedilen bilgi, makinenizdeki bir günce (log) dosyasına kaydedilir. Bu günce dosyası, önceden belirlenmiş bir zamanda, merkezi kaynağa aktarılır. Yazılımın göndermiş olduğu bilgiler daha sonra yasadışı yollarla satılabilir ve bu şekilde verileriniz kötü niyetli kişilerin eline geçebilir.

Casus yazılımlar sisteminize girdikten sonra aşağıdaki işlemlerden bazılarını ya da hepsini yapmaktadır; [34]

- Ziyaret ettiğiniz her bir web sayfasının adresini kaydetmek,
- E-posta gönderdiğiniz her alıcının adresini kaydetmek,
- Aldığınız her e-postayı gönderenin adresini kaydetmek,
- Aldığınız ya da gönderdiğiniz her e-postanın içeriğini kaydetmek,

- Bilgisayarınızın klavyesiyle yaptığınız her tuş vuruşunu kaydetmek,
- Farenizin hareketi ve işlemi dahil olmak üzere Windows ile ilgili bütün faaliyetlerinizi kaydetmek

4.2. Casus Yazılımların Belirtileri

Bilgisayarınıza bir casus yazılım bulaştığında bunu anlamanın farklı yolları vardır. Eğer bilgisayarınız daha öncekinden düşük performansta çalışıyorsa bu sisteminize bi casus yazılım bulaştığı anlamına gelebilir. Bir başka belirti de internet hızınızdaki düşüş olabilir. Casus yazılımlar düzenli olarak edindikleri bilgileri programcısı ile paylaştığı için internet ağınızda sürekli bir trafik oluşturur. Bunlar dışındaki bazı belirtiler aşağıdaki gibidir; [32]

- İnternette arama yaparken her amanki arama motorunuz yerine başka bir arama motoru üzerinden arama yapılıyorsa,
- İnternet tarayıcınnızın sık kullanılanlar bölümünde sizin kaydetmediğiniz siteler görünüyorsa,
- Sistem tepsinizde daha önce görmediğiniz bir program simgesi varsa,
- İnternet'e bağlantınız olmadığı durumlarda bile size adınızla hitap eden çıkıveren reklâmlar görüyorsanız,
- İnternet'e erişim olmadığı sırada sistem tepsisindeki ağ bağlantınızı gösteren (iki bilgisayar şeklinde gösterilen) simgede veri aktarımını gösteren hareketler görüyorsanız,
- CD sürücünüz kendi kendine açılıp kapanıyorsa,
- Rasgele hata mesajları alıyorsanız,

4.3. Casus Yazılımların Bulaşma Teknikleri

Casus yazılım programcılarının yazdıkları programı bir sisteme bulaştırmak için en büyük silahları e-posta adresleridir. Kullanıcılar bir reklam veya çekiliş kazandıklarına dair bir e-posta aldıklarını sanıp e-postadaki bağlantıya tıkladıklarında casus yazılım indirilir ve sisteme kurulur. Ardından bu program farkedilip temizlenene kadar programcısının istediği bilgileri kendisine iletir. E-postalardan sonra kullanılan en yaygın yöntemlerden biri ise lisanssız veya crackli programların içerisine eklenmiş casus yazılımların uygulama ile beraber yüklenmesi yöntemidir. Bunlar dışındaki yaygın yöntemler aşağıdaki gibidir;

- Bilgisayarınızı aldığınızda ilk kurulumu yapan kişinin bilerek ya da bilmeyerek casus yazılımı kurması,
- İnternet tarayıcılarında bulunan korunmasızlık ve açıklardan yararlanarak kurulum,
- Özellikle İnternet üzerinden kullanıcıya aldatıcı mesajlarla yanıltıp; her hangi bir casus yazılımın kurulumunun başlatılması,
- İşletim sisteminizde bir arka kapı oluşturulumuş olması,

4.4. Casus Yazılımların Türleri

Casus yazılımlar temelde sisteme gizlice sızan ve kendini belli etmeden çalışan programlardır. Ancak bazı yönlerden birbirlerinden ayrı isimlendirilmeleri gerekir. Genellikle yaptıkları işe göre isim alan casus yazılımlar aşağıdaki türlere ayrılır;

4.4.1. Reklam Yazılımı (Adware)

Adware veya diğer adıyla reklam yazılımı kullanıcının etkinliklerini takip eder ardından size ilgili reklamlar gösterir. Reklam yazılımları sadece kurulu oldukları makine üzerinde işlem yapar ve kendilerini kopyalamaya çalışmazlar. Bazı reklam yazılımları tarayıcınızın kontrolünü ele geçirerek yer işaretlerinizi, başlangıç sayfanızı ve arama motorunuzu sürekli değiştirebilir. Yazılım, reklamları statik kutu gösterimi, afiş gösterimi, tam ekran, video, açılır reklam veya başka bir biçimde dahil olmak üzere çeşitli şekillerde uygulayabilir. Reklam yazılımları şu şekillerde programcısına para kazandırır [18];

1. Tıklama başına ödeme: Reklamlara tıklandığında ödeme yapılır.
2. Görüntüleme başına ödeme: Reklam sizin karşınıza her çıktığında ödeme yapılır.
3. Yükleme başına ödeme: Reklam yazılımı ile beraber olan yazılım her yüklendiğinde ödeme yapılır.

Ad-Aware, Malwarebytes' Anti-Malware, Spyware Doctor ve Spybot – Search & Destroy dahil olmak üzere reklam görüntüleyen kötü amaçlı yazılımları algılamak, karantinaya almak ve kaldırmak için programlar geliştirilmiştir. Ayrıca, hemen hemen tüm ticari virüsten koruma yazılımları şu anda reklam yazılımlarını ve casus yazılımları algılar veya ayrı bir algılama modülü sunar [2].

Bazı reklam yazılımları kullanıcının bilgisi ve isteği dahilinde bilgisayarlara yüklenebilir. Bu tür yazılımlar kötü amaçlı yazılım olarak değerlendirilmezler. Kötü amaçlı reklam yazılımları en iyi ihtimalle, reklam yazılımı dikkatin dağılmasına ve iş akışının yavaşlamasına neden olur; en kötü ihtimalle, kişisel bilgileri izleyen ve kullanıcının izni veya bilgisi olmadan üçüncü taraflara ileten kod içerir [29].

4.4.2. Şifre Hırsızları

Şifre hırsızları bilgisayarınızda girdiğiniz tüm şifreleri kaydeder ve programcısına gönderir.

4.4.3. Numara Çeviriciler (Diallers)

Kullanıcının bilgisi olmadan ücretli numaraları arayarak mağduru maddi zarara uğratan yazılımlardır. Genellikle kabarık faturalar sonucunda farkedilir.

4.4.4. Bilgi Hırsızları

Bir bilgisayara veya başka bir cihaza bu tür casus yazılım bulaştığında, üçüncü taraflara parolalar, kullanıcı adları, e-posta adresleri, günlük dosyaları, tarayıcı geçmişi, sistem bilgileri, elektronik tablolar, belgeler, medya dosyaları vb. gibi

hassas bilgiler sağlayabilir. Bilgi hırsızları, kişisel verileri ve diğer hassas bilgileri toplamak için genellikle tarayıcı güvenlik açıklarından yararlanır.

4.4.5. Tarayıcı Ele Geçirme (Browser Hijackers)

Tarayıcı korsanları web tarayıcınızı kontrol eden bir casus yazılımdır. Eğer tarayıcı anasayfanızın, arama motorunuzun veya diğer ayarların sizin bilginiz dışında değiştiğini farkediyorsanız muhtemelen bir tarayıcı korsanına yakalanmışsınız demektir. Amaç, sizi spam reklam içeren istenmeyen sitelere yönlendirmektir. Bu programlar aynı zamanda veri madencileridir, tarama aktivitelerinizi kaydeder ve bilgileri reklamcılara satarlar. Tarayıcı korsanları, bankacılık bilgilerini ve diğer hassas verileri elde eden casus yazılım da içerebilir.

Bu yazılımlar ile genellikle görünür olmak amaçlanır. Örneğin, bu yazılımı kullanan kişi ya da kişiler, site ziyaret sayısını ve reklam gelirlerini artırmayı amaçlayabilir. Bu yüzden, bu sitelere zorunlu yönlendirme yapılır. Browser Hijacker, kullanıcıyı bilinmeyen adreslere yönlendirebilir. Böylece, daha önce ayarlanmış olan sayfalara kullanıcıları yönlendirerek reklam yapma amacı güder. Buradaki en büyük sıkıntı, yönlendirilen sayfaların ne kadar güvenli olduğunun belirsiz olmasıdır [7]. Bu web sayaları üzerinden bilgisayarınıza farklı ararlı yazılımlar bulaştırılabilir.

Bazı virüsten koruma yazılımları, kullanıcıları reklam yazılımlarının ve casus yazılımların varlığına karşı uyarır, ancak bazı yeni kötü amaçlı yazılımlar tespit edilemeyebilir veya güvenlik yazılımı davetsiz misafirin kökünü çözemeyebilir. Bu durumlarda, kullanıcıların arayüzün kontrolünü yeniden kazanmak için tarayıcılarını yeniden yüklemeleri gerekir. [25]

4.4.6. Klavye Dinleyiciler (Keyloggers)

Klavye dinleyiciler sizin bilgisayarda yaptığınız işlemleri kaydedip programcısı ile paylaşan programlardır. Klavye dinleyiciler ilk çıktıklarında sadc klavyenizde yapığınız tuşlamaları kaydemekteydi, ancak zamanla daha kompleks işlemleri de kaydetmeye başladılar. Klavye dinleyicilerin amacı kendini belli etmeden mümkün olduğunca uzun süre sistemde kalarak kullanıcının hareketlerini izlemektir. Klavye dinleyiciler genelde indirilen lisanssız programlar veya tanınmayan kaynaklardan gelen e-postalar aracılığıyla bulaşır.

Bu yazılımlar diğer kötücül yazılımlar gibi bilgisayarınıza zarar vermek amaçlı kullanılmazlar. Klavye dinleyiciler özellikle e-posta adresiniz ve şifreniz, kullanıcı adı ve şifreleriniz, banka hesap bilgileriniz, kredi kartı numaralarınız gibi kişisel verilerinizi çalmayı amaçlamaktadır. Bu tür bilgileri günlük adı verilen kayıtlarda tutarlar ve internete bağlandığınıda bu dosyayı şifreli bir şekilde programcısına gönderir. Programcı bu bilgileri internet üzerinden saışa çıkararak maddi kaanç sağlayabilir.

Klavye dinleyicilerin kötücül yazılım olarak tanımlanmayan farklı bir türü de mevcuttur. Bu tür kullanıcının bilgisi dahilinde bilgisayara yüklenen programlardır. Genellikle işverenler çalışanlarını veya ebeveynler çocuklarını kontrol etmek için bu tür klavye dinleyiciler kullanırlar.

Bilinen en eski keylogger aslında bilgisayar çağından daha eskidir. 1970'lerin ortalarında, Sovyetler Birliği, daktiloları hedefleyen bir donanım keylogger'ı

geliştirdi ve dağıttı. "Selectric bug" olarak adlandırılan bu cihaz, IBM Selectric daktilolarının yazıcı kafasının hareketlerini, yazıcı kafasının dönmesi ve hareketlerinin neden olduğu bölgesel manyetik alan üzerindeki ince etkiler yoluyla ölçtü. Casuslar bu cihazları Moskova ve Leningrad'daki ABD diplomatik tesislerindeki daktilolara entegre ettiler. [11]

Sisteminizde bir klavye dinleyici olduğunu farkettiyseniz o andan itibaren hiçbir şifrenizi kullanmadan bir anticasus programı ile casus yalımı silmeyi denemelisiniz. Eğer birkaç anticasus yazılım denemenize rağmen silmeyi başaramadıysanız en güvenli yöntem olarak bilgisayarınızı formatlamanız gerekebilir. Bir klavye dinleyicinin sisteminize bulaşmanızı istemiyorsanız işletim sisteminizi ve anticasus yazılımınızı sürekli güncel tutmanız gerekmektedir.

4.4.7. Yemleme (Phishers)

Türkçe'de yemleme veya oltalama olarak kullanılan bu saldırı türünün adı İngilizce şifre (password) ve balık avlamak (fishing) kelimelerinin birleşiminden türetilmiştir. Yemleme kötü amaçlar doğrultusunda bazı kurum ve kuruluşların, güvenli gibi görünerek kullanıcıların kredi kartı, kimlik bilgileri gibi hayati önem taşıyan kişisel verilerinin çalınmasını amaçlar. İnsan hatasına dayanan bu siber saldırılar aynı zamanda sosyal mühendislik saldırısı olarak da adlandırılır [14]. Yemleme saldırıları genelde ücretsiz tatil, para ödülü vb. ilgi çekici içeriklerle yapılır.

Saldırgan tarafından özel olarak hazırlanan phishing e-postası resmi bir kurumdan geliyormuş gibi ya da gerçek bir e-posta şeklinde görülür. İletilen e-posta mesajlarındaki zararlı bağlantılar tıklandığı zaman kurbanın av olması sağlanabildiği gibi e-postalar ile birlikte ek olarak gönderilen virüslü dosyaların çalıştırılması ile de kurbanların bilgisayarları saldırganlar tarafından ele geçirilebilir. [13]

Yemleme saldırıları kullanıcıların e-posta şifresi, kredi kartı ve banka hesap bilgileri gibi kişisel verilerini çalmayı amaçlar. Bu veriler maddi çıkar amaçlı kullanılabilir. Yemleme saldırılarından korunmak için aşağıdaki tedbirlere dikkat etmek gerekir; [15]

- Sözde Sistem Yöneticisi tarafından gönderilmiş gibi görünen ve e-posta kotanızın dolduğu gerekçesi ile şifre bilgilerinizi isteyen e-postalara cevap vermeyiniz, içerdiği bağlantıları tıklamayınız.
- Gelen e-posta'nın kimden geldiğinden emin değilseniz dikkate almayınız (Unutmayın hiç bir kurum veya kuruluş e-posta yoluyla sizden kişisel bilgilerinizi istemez).
- Şüpheli e-postaları, reklam ilan sayfalarını açmayınız, şüpheli bağlantıları ziyaret etmeyiniz. Bankalar, sosyal paylaşım siteleri, alış-veriş siteleri gibi bilinen bağlantılara internet tarayıcınızın adres çubuğuna hedef web adresini elle yazarak giriniz.
- Bilgisayarınızın güncellemelerini yapmayı ihmal etmeyiniz.
- Hesap şifrelerinizi yüksek güvenlikli olarak belirleyiniz (Büyük harf, küçük harf, sayılar ve diğer karakterlerden oluşan parola kullanımı ve en az 8-10 karakter).

4.5. Bazı Casus Yazılım Programları [12]

CoolWebSearch: Bir grup program olan CoolWebSearch, Internet Explorer güvenlik açıklarından yararlanır. Paket, trafiği coolwebsearch.com dahil olmak üzere Web sitelerindeki reklamlara yönlendirir. Pop-up reklamlar görüntüler, arama motoru sonuçlarını yeniden yazar ve DNS aramalarını bu sitelere yönlendirmek için virüslü bilgisayarın ana bilgisayar dosyasını değiştirir.

FinFisher: Bazen FinSpy olarak da adlandırılan FinFisher, kolluk kuvvetlerine ve istihbarat teşkilatlarına satılan üst düzey bir gözetim paketidir. Eğitim ve teknoloji güncellemeleri gibi destek hizmetleri paketin bir parçasıdır.

GO Keyboard: Kişisel bilgileri kullanıcıların açık izni olmadan uzak sunucularına iletir. Bu bilgiler, kullanıcının Google hesabı e-postasını, dilini, IMSI'sini, konumunu, ağ türünü, Android sürümünü ve yapısını ve cihazın modelini ve ekran boyutunu içerir. Uygulamalar ayrıca, Google Play gizlilik politikalarının Kötü Amaçlı Davranış bölümünü ihlal ederek uzak bir sunucudan bir kod indirir ve yürütür.

HuntBar: Nam-ı diğer WinTools veya Adware.Websearch, bağlı kuruluş Web sitelerinde bir ActiveX sürücüyle indirme yoluyla veya diğer casus yazılım programları tarafından görüntülenen reklamlarla kurulmuştur; casus yazılımların nasıl daha fazla casus yazılım yükleyebileceğinin bir örneğidir. Bu programlar Internett Explorer'a araç çubukları ekler, toplu tarama davranışını izler, bağlı kuruluş referanslarını yeniden yönlendirir ve reklamları görüntüler.

Internet Optimizer: DyFuCa olarak da bilinen Internet Optimizer, Internet Explorer hata sayfalarını reklamcılığa yönlendirir. Kullanıcılar bozuk bir bağlantıyı takip ettiğinde veya hatalı bir URL girdiğinde, bir reklam sayfası görürler. Ancak, parola korumalı Web siteleri (HTTP Temel kimlik doğrulama) HTTP hatalarıyla aynı mekanizmayı kullandığından, Internet Optimizer, kullanıcının parola korumalı sitelere erişmesini imkansız hale getirir.

Look2Me: Look2Me gibi casus yazılımlar, sistem açısından kritik süreçlerin içinde gizlenir ve güvenli modda bile başlatılır. Sonlandırılacak herhangi bir işlem olmadığında, hem casus yazılım hem de kök kullanıcı setinin bir kombinasyonu olan algılamaları ve kaldırmaları daha zordur. Daha yeni casus yazılım programlarının ayrıca iyi bilinen kötü amaçlı yazılımdan koruma ürünlerine karşı belirli karşı önlemleri olduğundan ve bunların çalıştırılmasını, kurulmasını ve hatta kaldırılmasını engelleyebileceğinden, kök kullanıcı takımı teknolojisi de artan bir kullanım görmektedir.

Zwangi: Zwangi, tarayıcının adres çubuğuna yazılan URL'leri www.zwangi.com, adresindeki bir arama sayfasına yönlendirir ve ayrıca izinsiz olarak ekran görüntüleri alabilir.

5. Zararli Yazilimlar

Zararlı yazılımlar veya bir diğer adıyla malware (malicious software) bilgisayar sistemine giren ve çalışmasını olumsuz etkileyen yazılımlardır. Bu isim Yisrael Radai tarafından 1990 yılında verilmiştir. Zararlı yazılım, bulaştığı bir bilgisayar sisteminde veya ağ üzerindeki diğer makinelerde zarara yol açmak veya çalışmalarını aksatmak amacıyla hazırlanmış istenmeyen yazılımların genel adıdır.[33]

Zararlı yazılımların amacı sisteminize girerek çalışmaz hale getirmek ya da içerisindeki kişisel verilerinizi çalmaktır. Eğer gerekli önlemleri almazsanız verileriniz bilgisayar korsanları tarafından ele geçirilir ve internette maddi çıkarları doğrultusunda sattışa çıkarılır. Diğer tür zararlı yazılımlar ise kişisel verilerinizi çalmak yerine sizi maddi zarara uğratmayı amaçlarlar. Bu yazılımlara fidye yazılımlar iyi bir örnektir. Fidye yazılımda bilgisayar korsanı bilgisayarınızdaki önemli bir dosyayı şifreler ve şifreyi kaldırmak için sizden para ister.

Zararlı yazılımlar ilk bulaşmalarını yaygın olarak bilinmeyen kaynaklardan gelen e-posta ekleri aracılığıyla yapar. Daha sonra bazı zararlı yazılımlar kendilerini ağ üzerinden kopyalayarak kurban sistem ile aynı aa bağlı olan tüm bilgisayarlara bulaşırlar. Bunun dışında eğer kurban bir sistemde harici veri depolama birimlerini (USB sürücü, harici hard disk vb.) kullanırsanız zararlı yazılımlar bu birimlere ve dolayısıyla da o birimlerin takıldığı diğer tüm bilgisayarlara bulaşır.

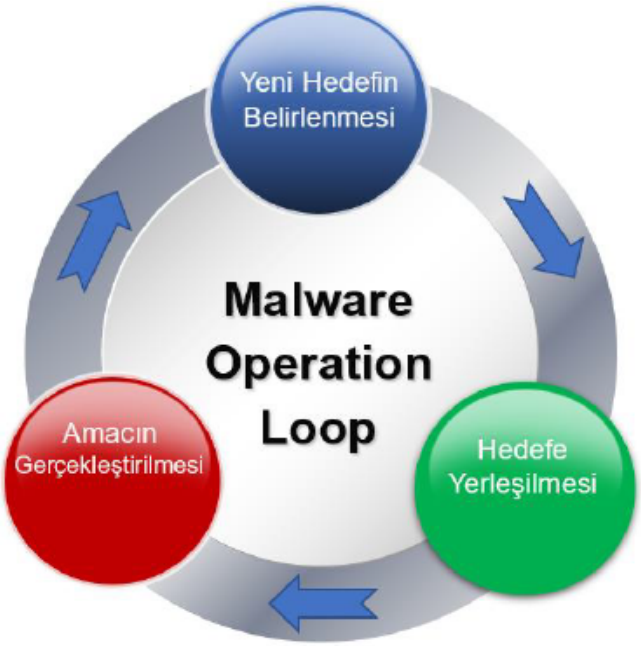
Zararlı yazılımların atası olarak örnek verebileceğimiz program bilgi güvenliğinin tarihçesi başlığı altında bahsettiğimiz Bob Thomas'ın 1971 yılında geliştirmiş olduğu "Creeper" isimli programdır. Creeper ağ içinde dolaşarak arkasında "I'm the Creeper : Catch me if you can" şeklinde bir yazı bırakmaktaydı ancak hiçbir veriye zarar vermemiştir. Bundan bir yıl sonra 1972 yılında Ray Tomlinson isimli bir bilgisayar programcısı Creeper'ı bulup silebilen ve ağ içerisinde gezebilen bir program yazdı. "Reeper" isimli bu program tarihteki ilk antivirüs olması ve ağ içerisinde gezip kendi kendini kopyalayabilmesi özelliği ile ilk bilgisayar solucanı olması açısından önemlidir.

5.1. Zararlı Yazılımlar Nasıl Çalışır

Zararlı yazılımların öncelikli amacı kendini başka sistemlere kopyalayarak etki alanını arttırmaktır. Bir zararlı yazılım sisteminize bulaştıktan sonra yapması için programlandığı şeyi yapar (dosyalarınızı silme, dosyalarınızı şifreleme vb.). Daha sonra kendini e-posta veya ağ yoluyla kopyalayabildiği kadar kopyalar ve yayılmaya çalışır. 5.1'da zararlı yazılımların işleyiş döngüsü bulunmaktadır.

5.2. Zararlı Yazılımların Belirtileri

Eğer bilgisayarınıza bir zararlı yazılım bulaştıysa bunu casus yazılımlara benzer şekilde anlayabilirsiniz. Casus yazılımlardan farklı olarak zararlı yazılımlar bilgisayarınızdaki dosyalarda değişiklikler yapabilirler. Dosyalarınızın isimlerinde veya boyutlarında sizin etkiniz olmadan değiştiyse muhtemelen bir zararlı yazılım dosyalarınıza müdahale ediyor demektir. Ayrıca zararlı yazılımları tespit etmenin



Şekil 5.1 Zararlı yazılımların işleyiş döngüsü (Malware's operating loop) [26]

bir başka yolu da dosyalarınıza yaptığı gibi web tarayıcınızın ayarlarıyla oynaması da olabilir. Bazı zararlı yazılımlar web tarayıcınızın açılış sayfasını ve yer işaretlerine kayıtlı sayfaları değiştirebilir. Bunları dışında kalan zararlı yazılım belirtileri ise aşağıdaki gibidir;

- Bilgisayarınız normalden daha yavaş çalışmaya başladıysa,
- İnternet hızınız çok düştüyse,
- Web tarayıcınız kendi kendine bazı sitelere girmeye çalışıyorsa,
- Sıklıkla bunları düzeltmek için bir şeyler satın alma talepleriyle birlikte gelen enfeksiyon uyarıları alıyorsanız,
- Bilgisayarınız açılıp kapanırken zorlanıyorsa,
- Sıklıkla bunları düzeltmek için bir şeyler satın alma talepleriyle birlikte gelen enfeksiyon uyarıları alıyorsanız,
- Dosya bilgileri değişir [36].

5.3. Zararlı Yazılımların Bulaşma Teknikleri

Zararlı yazılımlar genelde veri depolama birimleri ile yapılan dosya alışverişleri sırasında bulaşırlar. Eğer bilgisayarınıza taktınız bir USB veya CD sürücüde zararlı yazılım bulunuyorsa bu zararlı yazılım bilgisayarınıza da bulaşacaktır. Bunun dışında yine casus yazılımlarda olduğu gibi e-postaların içerisinde bulunan bağlantı veya ekler aracılığıyla da sisteminize zararlı yazılım bulaştırılabilir. Bunlar dışında kalan bulaşma teknikleri ise şu şekildedir;

- Gezindiğiniz web sitesindeki reklamlara zararlı yazılım entegre edilmesi,
- Güvenilir web sitelerinin hacklenmesi ve içerisine zararlı yazılım eklenmesi,
- İnternetten indirdiğiniz dosyaların içerisinde zararlı yazılım bulunması,

5.4. Zararlı Yazılımların Türleri

Zararlı yazılımlar ilk ortaya çıktıklarında genel olarak bilgisayar virüsü ismiye anılıyordu. Ancak daha sonra geliştirilen ve farklı işlevlere sahip olan programlar da zararlı yazılım olarak sistemlere bulaşmaya başladı. Bu yeni geliştirilen zararlı yazılımlara yaptıkları işlerden esinlenilerek yeni isimler verilmeye başlandı. En yaygınları virüs, solucan ve truva atı olan bu türler aşağıdaki gibidir;

5.4.1. Virüsler

Bilgisayar virüsleri de biyolojik virüsler gibi bulaştığı sistemi kullanılamaz hale getirir ve bu sistemi kendini çoğaltmak için bir araç olarak kullanır. Daha önceki yıllarda donanıma zarar verebilen virüsler mevcuttu ancak donanımlar kendilerini virüslere karşı geliştirdi ve artık virüsler donanımlara zarar veremiyor[37]. 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. Virüsleri diğer zararlı 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[33].

Bilgisayar virüslerinden korunmak için işletim sisteminizin güncel olduğundan ve güvenilir bir antivirüs programı kulandığınızdan emin olmalısınız. Eğer bir harici veri depolama birimi kullanıyorsanız bu birimi her kullanımınızda taramanız yararlı olacaktır. Bu önlemlerin yanında bilgisayarınızda virüs olmadığınızdan emin olduğunuz bir zamanda bilgisayarınızda geri yükleme noktası oluşturmalısınız. Bu şekilde eğer bilgisayarınıza virüs bulaşştıysa formatlamayya gerek kalmadan bu noktaya dönerek virüsten kurtulabilirsiniz.

Bilgisayarınıza bir virüs bulaştıysa bunu anlayabileceğiniz birkaç belirti mevcut. Depolama alanınızın normalden daha az görünüyorsa, bir program yüklemeye çalışırken uzun sürüyorsa, ekranınızda bir anda reklamlar çıkıyorsa ve ayarlarınızda bilginiz dışında değişiklikler oluyorsa muhtemelen bilgisayarınıza virüs bulaşmıştır.

Virüsleri şu şekilde sınıflandırabiliriz;
Dosya virüsleri: En yaygın bilgisayar virüslerinden biridir. Çalıştırıldığı zaman dosyanın üerine yazar veya dosayaya zarar verir. En yaygın bulaşığı dosya türleri .exe ve .com uzantılı dosyalardır. Birçok dosya virüsü kendilerini sistem hafızasına yükleyip sürücüdeki diğer programları araştırarak yayılır. Bulduğu programların kodlarını virüsü içerecek ve gelecek sefer program çalıştığında virüsü de etkinleştirecek şekilde değiştirir. Virüs tüm sisteme ya da bulaştığı programı ortak

kullanan sistemlerin tüm alanlarına yayılana dek defalarca bunu yapar.

Önyükleme (boot) virüsleri: 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. Önyükleme sektörü virüsüne karşı koruma adımları, disklerin yazmaya karşı korumalı olmasını sağlamayı ve güvenilmeyen harici sürücülerin bağlı olduğu bir bilgisayarı başlatmamayı içerir.

Makro virüsleri: Makro dillerini destekleyen Microsoft Office(Word,Excel,PowerPoint) programlarını kullanarak yayılan virüslerdir. Bu tür virüsler makrolar ile birikte Linux, Windows ve MacOS işletim sistemlerinde akti hale getirilebilirler.

Betik (script) virüsleri: Betik dilleri (Visual Basic, JavaScript, PHP vb.) kullanılarak yazılan virüslerdir. Genelde HTML dosyalarına yapışırlar ve bu dosyalar açıldığında aktif olurlar.

Ağ virüsleri: Tüm bilgisayar ağlarını aynı anda çökertebilecek bir virüs türüdür. Çoğalmak için bağlı olduğunuz tüm ağdaki bilgisayarlara kendini kopyalar. Bu virüs ağınızda bulunan tüm bilgisayarda saklanabileceği için bulup silmesi çok zordur.

Sentineller: Sentineller oldukça gelişkin virüs tipi olup yaratıcısına, bulaştığı bilgisayarları uzaktan kullanma yetkisi verir. Sentineller bot, zombi ya da köle adı verilen bilgisayarların oluşturduğu ve Hizmeti engelleme saldırısı gibi kötü niyetli amaçlarda kullanılacak geniş ağlar yaratmada kullanılırlar. [5]

DOS virüsleri: DOS virüsleri, isminini Windows XP sürümüne kadar eski Windows sürümlerinin üstüne yapıldığı DOS işletim sisteminden alır. Bilgisayara donanımsal zarar veren tek virüslerdir. Kendileri Windows'un Batch özelliğini kullanır. Uzantısı .bat biçimindedir ama her .bat uzantılı dosyalar virüs değildir. Küçük boyutlu olan bu virüsler genellikle açıldığı anda işleme koyulurlar. Küçük olmasının nedeni aslında sadece bir yazı dosyası olmasından kaynaklıdır. Windows, o .bat uzantılı dosyadaki yazı komutları çalıştırır. .bat dosyalarının formatı cmd.exe'ye komut yazarmış gibidir. [5]

5.4.2. Truva Atları

Adı eski Yunan efsanelerinden olan Truva Savaşı mitinden türemiştir.Bir diğer adı trojandır. Zararsız yazılım güncellemeleri veya e-posta ekleri olarak gizlendikleri için truva atları olarak adlandırılırlar. Bu terim ilk kez 1974 ABD Hava Kuvvetleri raporunda zararlı kodları tanımlamak için kullanıldı [23].

Truva atlarının aktif hale gelmesi için kurban tarafından çalıştırılması gerekmektedir. Truva atları kendilerini bir başka sisteme kopyalamayı başarsa bile yeni kurban truva atını çalıştırmadan aktif hale geçmez. Bu yönüyle truva atlarının

kullanımı yoğun bir sosyal mühendislik bilgisi gerektirmekedir.

Truva atları sisteminize birkaç şekilde zarar verebilirler. Bunlardan birkaçı;

- Sisteminizde arka kapı açabilirler,
- Verilerinizi silebilir, değiştirebilir veya şifreleyebilirler,
- Güvenlik yazılımınızı devre dışı bırakabilirler,
- Sizin bilginizz dışında e-posta gönderebilirler,
- İnternet erişiminize zarar verebilirler.

Truva atlarının iki türü vardır. Birincisi, kullanışlı bir programın bir hacker tarafından tahribata uğrayıp içine zararlı kodlar yüklenip program açıldığında yayılan cinsi. Örnek olarak çeşitli hava durumu uyarı programları, bilgisayar saati ayarlama yazılımları ve paylaşım programları verilebilir. Diğer türü ise bağımsız bir program olup başka bir dosya gibi görünür. Örneklemek gerekirse oyun veya kalıp dosyası gibi kullanıcıyı aldatmaya yönelik bir takım yönlendirici karışıklık ile programın harekete geçirilmesine ihtiyaç duyulmaktadır. Trojan virüslerini yapmaya yarayan programlar bulunmaktadır. [22]

Java veya Flash oynatıcı güncellemeleri, casus yazılımları teslim etmek için yaygın olarak truva atı olarak kullanılır. Truva atları diğer kötücül yazılımların aksine kendi başlarına işlem yapamazlar. Kullanıcı programı çalıştırmadığı sürece aktif hale gelmezler.
azı ruva aı ürlerini şu şkilde sıralayabiliriz;

1. **Arka Kapı Truva Atları:** Sisteminize uzaktan erişim sağlayabilecek bir arka kapı oluşururlar. Bu arka kapı sayesinde bilgisayar korsanları siseminize başka zararlı yazılımlar yükleyebilirler, verilerinizi çalabilirler ve dosyalarınızı silebilirler. Ayrıca bu truva atları sayesinde bilgisayarınız saldırıya hazır bir zombi bilgisayar ağının parçası olurlar.

2. **Rootkit:** Rootkit'ler, sisteminizdeki belirli nesneleri veya etkinlikleri gizlemek üzere tasarlanmıştır. Bunların başlıca amacı, genellikle kötü amaçlı programların algılanmasını önleyerek programların virüslü bir bilgisayarda çalışacağı süreyi uzatmaktır.

3. **Bankacılık Truva Atları:** Bankacılık ruva aları kullanıcının banka bilgilerini ele geçirmek için tasarlarnmış truva atarıdır. Bunu yapmak için potansiyel kurbanları, erişim kimlik bilgilerini girmeleri gereken değiştirilmiş bir sayfaya göndermek gibi kimlik avı tekniklerini kullanırlar.

4. **DDoS Truva Atları:** Bu truva atı bulaştığı tüm bilgisayarları kullanarak bir hedefe DDoS saldırısı yapmak için kullanılır. Bu truva atı sistemde kendini

farkettirmeden çalışır ancak arkaplanda programcısının emirleri doğrultusunda saldırılar için kullanılır.

5. **Yazılım yükleyici/indirici Truva Atları:** Bu ruva atları siseminize daha fazla zararlı yazılım indirip kurmaya çalışırlar.

6. **Fidye Truva Atları:** Bu tür Trojanlar, bilgisayarınızdaki verileri değiştirerek bilgisayarın doğru çalışmamasına veya belirli verilerin kullanılamamasına yol açar. Suçlu, fidye isteğinde bulunur ve ancak bu paranın ödenmesi karşılığında bilgisayar performansını eski haline getirir veya verilerinizin üzerindeki engeli kaldırır.

5.4.3. Solucanlar

Bir diğer adı worm'dur. 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[33]. Solucanlar veri kaybına ve sistem hasarına neden olmazlar.

Solucan virüsü, kendisini bir bilgisayardan başka bir bilgisayara kopyalamak için tasarlanmıştır ve bu işlem otomatik olarak gerçekleşir. İlk olarak bilgisayarda dosya veya bilgi ileten özelliklerin denetimini ele geçirir. Solucan sisteminize girdikten sonra kendi başına ilerleyebilir. Örneğin; bir solucan, e-posta adres defterindeki herkese kopyalarını gönderebilir ve aynı şeyi onların bilgisayarları da yapabilir. Bu, domino etkisinin getirdiği yoğun ağ trafiği, iş yeri ağları ve internetin tümünü yavaşlatabilir. Yeni solucanlar ilk ortaya çıktıklarında çok hızlı yayılırlar ve ağları kilitleyerek web sitesi ziyaretlerini yavaşlatabilirler. [19]

Bilgisayar virüsleriyle solucanlar arasındaki önemli bir ayrım, virüslerin çalışması, zarara neden olması ve diğer yürütülebilir dosyalara veya belgelere bulaşması için aktif bir ana program ya da halihazırda virüs bulaşmış ve aktif bir işletim sistemi gerekirken solucanların kendisini kopyalayabilen ve insan yardımı olmadan bilgisayar virüsleri yoluyla çoğalabilen bağımsız kötü amaçlı programlar olmasıdır. Solucanların çalışması, kendini kopyalaması ve çoğalması içinse ana program gerekmez. Bir solucan genellikle ağ bağlantısı veya indirilen bir dosya yoluyla sisteminize girdikten sonra ağ veya internet bağlantısı üzerinden kendisinin birden fazla kopyasını yapıp yayılarak ağdaki yeterince korunmayan tüm bilgisayarları ve sunucuları etkiler. Ağ solucanının birbirini izleyen her bir kopyası da kendi kendine çoğalabildiği için virüsler internet ve bilgisayar ağları yoluyla hızla yayılabilir. [6]

Yararlı bir solucan veya anti-solucan, mutlaka yürüten bilgisayarın sahibinin izniyle olmasa da, yazarının yararlı olduğunu düşündüğü bir şeyi yapmak için tasarlanmış bir solucandır. Xerox PARC'ta solucanlar üzerine yapılan ilk araştırmadan başlayarak, faydalı solucanlar yaratmaya yönelik girişimlerde bulunuldu. Bu solucanlar, John Shoch ve Jon Hupp'un Xerox Alto bilgisayar

ağlarında Ethernet ilkelerini test etmelerine izin verdi. Benzer şekilde, Nachi solucan ailesi, aynı güvenlik açıklarından yararlanarak ana bilgisayar sistemindeki güvenlik açıklarını düzeltmek için Microsoft'un web sitesinden yamalar indirip yüklemeye çalıştı. Pratikte bu, bu sistemleri daha güvenli hale getirmiş olsa da, önemli miktarda ağ trafiği oluşturdu, yama sırasında makineyi yeniden başlattı ve çalışmasını bilgisayar sahibinin veya kullanıcısının izni olmadan yaptı. Yükleri veya yazarlarının niyetleri ne olursa olsun, güvenlik uzmanları tüm solucanları kötü amaçlı yazılım olarak görür. [8]

5.4.4. Bot

Bot'lar kendi başlarına bilgisayara zarar vermezler. Ancak bir kullanıcı gibi kendisinden yapılması istenen şeyi yaparlar. Bunlar da kullanıcıdan izinsiz program veya zararlı yazılım indirmek gibi şeyler olabilir. Genelde toplu saldırılarda kullanılırlar.

5.4.5. Fidye Yazılımları

Fidye yazılımlar bilgisayarınızdaki bazı dosyaları şifreleyerek bunları erişiminize açmak için para isteyen yazılımlardır. Çoğu durumda, fidye yazılımlarının bilgisayara girişi şu şekilde olur. İlk olarak kötü amaçlı yazılım cihaza erişim kazanır. Fidye yazılımının türüne bağlı olarak, işletim sisteminin tamamı ya da belirli dosyalar şifrelenebilir. Sonrasında kurbanlardan bir fidye talep edilir. [10] Bu para daha önceleri normal para birimleri ile istenmekteydi. Ancak bu tip paraların takip edilebilir olmasından dolayı artık kripto para birimleri istenmektedir. İki tip fidye yazılımı kullanılmaktadır[28].

Locker Fidye Yazılım: Bilgisayarın veya aygıtın kilitlendiği fidye yazılım türüdür.

Crypto Fidye Yazılım: kişisel dosyaların şifrelendiği fidye yazılım türüdür.

Fidye yazılımların öncüsü 1989 yılında Joseph Popp tarafından yazzılan program olarak kabul edilmektedir. Ancak bu program bir tasarım hatasından dolayı fidye ödenmesini gerekli kılmıyordu. PC Cyborg olarak bilinen bu program 'PC Cyborg Corporotion'a 189 dolar fidye ödenmesini istiyordu. Asıl fidye yazılımı olarak ifade edebileceğimiz yalımlar ise 2005 yılında Rusya'da ortaya çıktı. 2018'in ilk altı ayında 181,5 milyon fidye yazılımı saldırısı gerçekleşti. Bu rekor, 2017'de aynı zaman dilimine göre %229'luk bir artışa işaret ediyor. [17] Haziran 2014'te, satıcı McAfee, o çeyrekte bir önceki yılın aynı çeyreğine göre iki kattan fazla fidye yazılımı örneği topladığını gösteren verileri yayınladı. [16]

Locker Fidye Yazılım: Bilgisayarın veya aygıtın kilitlendiği fidye yazılım türüdür.

Crypto Fidye Yazılım: kişisel dosyaların şifrelendiği fidye yazılım türüdür.

5.4.6. Spam

Mesaj sağanağı olarak da bilinen spamlar genede reklam ve çeşitli zararlı sitelere yönlendirme yapmak için kullanılan bir zararlı yazılımdır. Mail yoluyla toplu olarak aynı mailin gönderilmesi olayıdır. Spamlar kendi başlarına bir zarar vermeseler de

içerisinde bulunan linklere tıklanması halinde sisteme sızılmasına neden olunabilir.

5.4.7. Arka Kapı (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[33].

5.5. Bazı Zararlı Yazılım Programları

ILOVEYOU: 2000 yılında Reonel Ramones ve Onel de Guzman tarafından gelişirilen bu zararlı yazılım e-posta aracılığıyla sahte bir aşk mektubu göndermekteydi. Daha sonra kurbanın adresinde kayıtlı tüm e-posta adreslerine aynı mektubu gönderme işlemini tekrarlayarak kendini daha fazla bilgisayara bulaştırmıştır. Dünya çapında 10 ila 15 milyar dolar zarara uğratttığı tahmin edilmektedir.

Code Red: Bu zararlı yazılım Microsoft IIS serverlarına ve Beyaz Saray web sayfasına saldırıda bulunmuştur. Beyaz Saray bu yazılımdan kurtulmak için IP adresini değiştirmek zorunda kalmıştır.

Melissa: David L. Smith tarafından 1999 yılında yaratılmıştır. İçerisinde yetişkin içerikli siteler için şifreler bulunduğunu iddia eden bir Word belgesi aracılığı ile bulaşmıştır. Kendisini kurbanın e-posta adresine kayıtlı ilk 50 kişiye otomatik olarak göndermiştir. Bu işlem dolayısıyla e-posta servislerinde aksamalara neden olan Melissa virüsünün 80 milyon dolar zarara neden olduğu düşünülmektedir.

Storm : 2007 yılında Avrupa'da fırtına içerikli haber başlıkları ile gönderilen e-postalar aracılığıyla yayılmıştır. Güzel bir sosyal mühendislik örneği olan bu zararlı yazılım insanların merakını kullanarak Avrupa ve Amerika'da 1 milyon bilgisayara bulaşmıştır.

Sasser: 2004 yılında 17 yaşında bir Alman öğrenci olan Sven Jaschan tarafından geliştirilen bu zararlı yazılım milyonlarca bilgisayara bulaşıp sistemlere zzarar vererek yaklaşık 18 milyar dolar zarara neden olmuştur.

My Doom: 2004 yılında geliştirilen bu solucan ILOVEYOU ile birlikte en hızlı yayılan zararlı yazılımlardan biridir. Solucanı kimin geliştirdiği bilinmemektedir. Solucan, bir e-posta iletim hatası olarak görünerek kendini yayar ve kendi ekini içerir. Yaklaşık 38.5 milyar dolar zarara neden olmuştur.

Conficker: Bir solucan olan Conficker yazılımı 190 ülkede 9 ila 15 milyon bilgisayara bulaşmıştır. Botnet oluşturmak için işletim sistemindeki kusurları kullanarak bilgisayarlara bulaşır. Hesap kilitleme ayarlarını sıfırlar ve virüsten

koruma sitelerine ve Windows güncellemelerine erişimi engeller. Daha sonra kullanıcı hesaplarını kilitler.

Stuxnet: İsrail ve Amerikan savunma güçleri tarafından İran'ın nükleer programlarını sekteye uğratmak için geliştirilmiştir. İyi bir siber savaş örneğidir.

CryptoLocker: CryptoLocker en etkili fidye yazzılımlarından biridir. Kendini yaymak için e-posta gibi çeşitli yöntemler kullanır ve bir bilgisayara virüs bulaştığında, sabit sürücüdeki ve ona bağlı herhangi bir takılı depolama birimindeki belirli dosyaları RSA ortak anahtar şifrelemesi ile şifrelemeye devam eder. Bu yazılımdan kurtulmak için kendisini temizlemek yetmez çünkü dosyalarınız şifreli kalmaya devam edecektir. Bu durumdan kurtulmak için yaklaşık 27 milyon dolar ödeme yapıldığı tahmin edilmektedir.

Wannacry: Bir başka fidye yaızlım örneği olan Wannacry 99 ülkede 230.000 bilgisayara bulaşmıştır. Bitcoin aracılığı ile ödeme yapılmasını isteyen Wannacry 51.62396539 Bitcoin (130.634,77 ABD Doları) tutarında öödeme almıştır.

6. Casus ve Zararli Yazilimlardan Korunma Yöntemleri

Bu tür yazılımlardan korunmanın en etkili yöntemi internet üzerinden yaptığınız işlemlere dikkat etmektir. İnternette gezindiğiniz sitelerde çıkan pop-up pencerelerindeki uyarıları onaylamanız halinde bu yazılımlar bilgisayarınıza yüklenir. Bu uyarılarda ilginizi çeken reklam veya zararsız görünen yazılımların bulunması sizi kuşkulandırmamak için yapılan bir hiledir. Ayrıca internetten indirdiğiniz crackli veya ücretsiz programları kurarken aynı zamanda bu programlara entegre edilmiş casus ve zararlı yazılımları da kurmuş olursunuz. Sosyal mühendislik denilen bu yöntemler sayesinde bilgisayar korsanları kullanıcıları kolaylıkla kandırarak bu tür yazılımları bilgisayarlara yüklemekte ve kullanmaktadır. Bu bölümde bu tür durumların önüne geçmek için almanız gereken önlemler incelenmektedir.

6.1. Casus Yazılımlardan Korunma Yöntemleri

Casus yazılımlardan korunmanın en etkili yöntemi anti-casus yazılımlar kullanmaktır. Bu yazılımlar bilgisayarınızda bir casus yazılım olup olmadığını taramanıza ve eğer varsa silmenize yardımcı olan programlardır. Ancak ilk bakışta çok iyi ve yararlı gibi görünen bu yazılımları bilgisayarınıza yüklemeden önce dikkatli olmalısınız. Çünkü bu yazılımları bir sosyal mühendislik malzemesi olarak gören bilgisayr korsanları anti-casus yazılım gibi görünen ancak tam aksine bir casus yazılım gibi çalışan programlar üretmektedirler. Bundan dolayı bu tür programları yüklemeden önce internette detaylı araştırılmalı veya bir uzmandan yardım alınmalıdır.

Anti-casus yazılımı kullanmadan bu casus yazılımlardan korunmak da mümkündür. Bu yöntemler aşağıdaki gibidir [32];

- İşletim sisteminizin güncel olduğundan emin olun,
- Elinizden geldiğince lisanslı yazılımlar kullanmaya çalışın böylece hem crack programı ile birlikte casus yazılımı bilgisayarınıza yüklememiş olursunuz hem de gerektiğinde ilgili programın destek biriminden yardım alabilirsiniz,
- Bilgisayar korsanları daha çok İnternet Explorer tarayıcısı üzerinden saldırmaktadır. Bundan dolayı Firefox, Opera veya Chrome gibi dier ücretsiz tarayıcılar tercih edilebilir,
- Umuma açık yerlerdeki (internet kafe, üniversite yerleşkesi vb.) bilgisayarlar üzerinden kredi kartı veya banka hesap bilgileri gibi önemli bilgilerinizi içeren işlemleri yapmamalısınız,
- Bilgisayarınıza bir firewall programı kurun,
- Windows Defender özelliğini aktif halde tutun.

6.2. Zararlı Yazılımlardan Korunma Yöntemleri

Zararlı yazılımlardan korunmanın en etkili yolu antivirüs programlarıdır. Bu programlar anti-casus yazılımların yaptığı gibi sisteminizi tarar ve zararlı yazılım

tespit ederse sizi uyarır ve silmenize yardımcı olur. Ancak bu tür programları kullanırken dikkatli olmak gerekir. Kötü amaçlı yazılımcılar kullanıcıların bu ihtiyacını kendi lehlerine kullanmak için sahte antivirüs denilen adı verileen yazılımlar geliştirmişlerdir. Gerçekte bilgisayarınıza zarar vermek amacıyla yazılmış fakat kendilerini birer virüs koruma yazılımı, tam sistem koruma yazılımı, casus yazılım engelleme aracı olarak gösteren bu tür yazılımlar aslında birer sahte antivirüs programıdır. Aynı bir antivirüs programı gibi davranır, bilinçsizce ya da yanlışlıkla tıklanan bağlantı ile bilgisayara bulaşır. Bilgisayar tekrar baştan başlatıldığında(boot) aktif olur. Bu sahte antivirüs programları, bilgisayarımızda birçok virüsün bulunduğu ve bunları temizlemenin tek yolunun da kullanmakta olduğumuz antivirüs programının ücretli sürümünü indirmekten geçtiği konusunda ekranımızı ısrarcı uyarı mesajlarıyla doldurur [36]. Bu nedenden dolayı bir antivirüs programı kullanırken bu programın piyasada kabul görmüş güvenilir bir program olmasına dikkat edilmelidir.

Antivirüs programı kullanmadan zararlı yazılımlardan korunabileceğiniz diğer yöntemler şu şekildedir;

- İşletim sisteminizin tüm güncellemelerinin yapılmış olduğundan emin olun,
- Tanımadığınız adreslerden gelen e-postaların içerisinde bulunan ekleri indirmeyin ve bağlantıları tıklamayın,
- İnternetten indirdiğiniz ve lisanslı olmayan programları kurarken Windows Defender uygulamasının vey muadili bir programın aktif olduğundan emin olun,
- Bilgisayarınıza taktığınız harici veri depolama birimlerinin temiz olduundan emin olun veya bir program kullanarak tarayıp daha sonra kullanın,
- Bilgisayarınıza güvenilir bir firewall programı kurun,
- İnternette gezindiğiniz sitelerin güvenlik onaylı olduğundan emin olun,
- İnternet üzerinden yaptığınız dosya paylaşımlarında güvendiğiniz siteleri kullanın.

7. Örnek Uygulama

Yapılan bu uygulama fidye yazılımlarına bir örnek olması amacı ile. Şifreleme yapmak için Pytohn programlama dilinde base64 kütüphanesi kullanılmıştır. Uygulama hedef bilgisayarda istenilen konumdaki dosyaları .txt formatına çevirip daha sonra bu dosyaların içeriğini base64 algoritması ile şifrelemektedir.

Uygulama içerisindeki dosya işlemlerini yapmak için ise os modülü kullanılmıştır. Bu kütüphanenin walk fonksiyonu sayesinde uygulama çalışması istenen dizine yöneltilmiştir. Bu fonksiyon uygulamanın istediğimi dizinde çalışmasını sağlamaktadır. İstenilen dizine ulaştıktan sonra os.path.splitext fonksiyonu ile o konumda bulunan tüm dosyaları .txt formatına çevirme işlemi yapılmıştır. Daha sonra ise bu çevrilen dosyaların içerikleri base64 algortiması ile şifrelenmiştir.

Kullanılan kütüphanelerin ve işlemlerin detaylı açıklamaları ise şu şekildedir.

7.1. Base64 Kütüphanesi

Base64 algoritması ASCII karakterleri kullanarak şifreleme yapan bir algoritmadır. Adı sayısal olarak ifade edilebilen 64 karakter olmasından gelmektedir. Bu karakterler 26 büyük harf, 26 küçük harf, 10 rakam, + ve / karakterleridir. Bu karakterler ve ondalık karşılıkları Şekil 7.1 belirtilmiştir.

Base64 Encoding Table

Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

Şekil 7.1 Base64 algoritmasında kullanılan karakterlerin onluk sayı sistemindeki değerleri [4]

Şifreleme işlemini yapmak için kütüphanenin b64encode fonksiyonu kullanılmıştır. Base64 algoritmasının adımları şu şekildedir.

1. Şifrelenmesi istenen metindeki her karakterin ASCII tablosundaki karşılıkları alınır.
2. Alınan bu verilerin 8 bitlik ikili sayı sistemindeki karşılıkları bulunur.
3. Bu 8 bitlik veriler 6'şar bitlik gruplara ayrılır.
4. Bu 6 bitlik veriler ondalık sayı sistemindeki sayılara dönüştürülür.
5. Son olarak ortaya çıkan bu verilerin ASCII tablosundaki karşılıkları alınır ve şifrelenme tamamlanmış olur.

7.2. Os Modülü

İşletim sistemlerinin çalışma mantıı birbirlerinden farklıdır. Ancak tüm işletim sistemlerinde çalışabilmeyi amaçlayan Python dilinde bu farklılıkları gidermek için os modülü kullanılır. Os modülü ile işletim sistemi içerisinde dizinlere ve dosyalara erişim sağlanabilmektedir. Bu uygulamada kullanılan os modülü fonksiyonları şunlardır;

os.walk(): Bu fonksiyon istenilen dizine gidilmesinin ve içerisindeki tüm alt dizinlere erişilmesini sağlar.

os.path.join(): Bu fonksiyon verilen dizinin farklı işletim sistemlerine uyun hale getirilmesini sağlar.

os.path.splitext(): Bu fonksiyon dosyanın adı ile uzantısının birbirinden ayrılmasını sağlar. Uygulama içerisinde bu fonksiyonun 0. indeksini yani dosya adını alıp .txt uzantısını ekleyerek dosyaların uzantısı değiştirilmiştir.

7.3. Uygulama Kodları

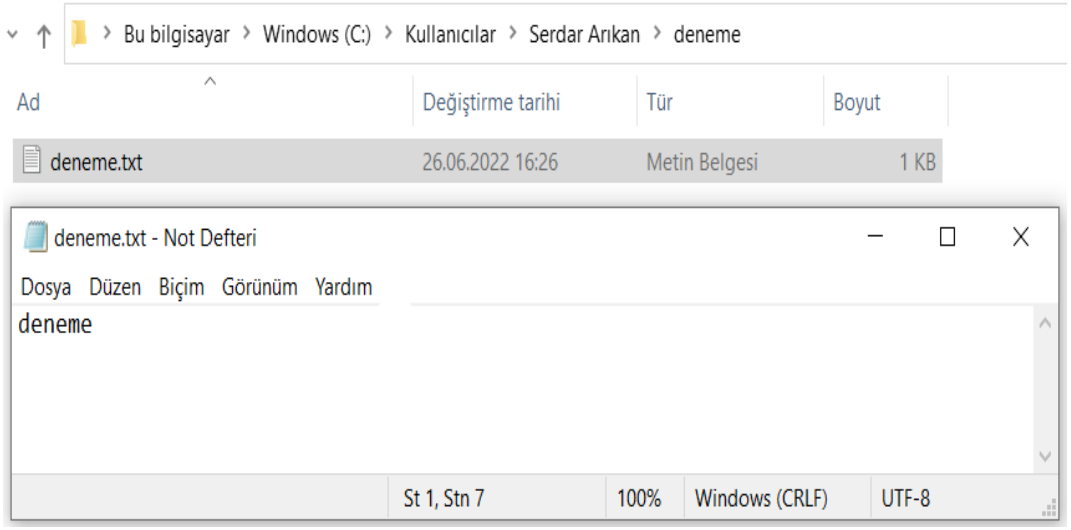
```
import base64
import os
liste = []
files = []

for r, d, fa in os.walk('C:/Users/serdar/deneme'):
    for file in fa:
        files.append(os.path.join(r, file))
for f in files:
    dosyaOkuma = open(f, 'rb').read()
    dosyaEncode = base64.b64encode(dosyaOkuma).
    decode('UTF-8')
    os.remove(f)
    f=(os.path.splitext(f)[0]+'.txt')
    with open(f, "w") as file:
        file.write(str(dosyaEncode))
    with open(f, "r") as fa:
        liste = [i for i in fa.readlines() if i
        is not None or len(str(i).strip()) > 0]
    with open(f, "w") as fa:
        for x in liste:
            encoded = x.encode()
            sifreleyici = base64.b64encode(encoded)
            mesaj = sifreleyici.decode()
            x = x.replace(x, mesaj)
            fa.write(x)
```

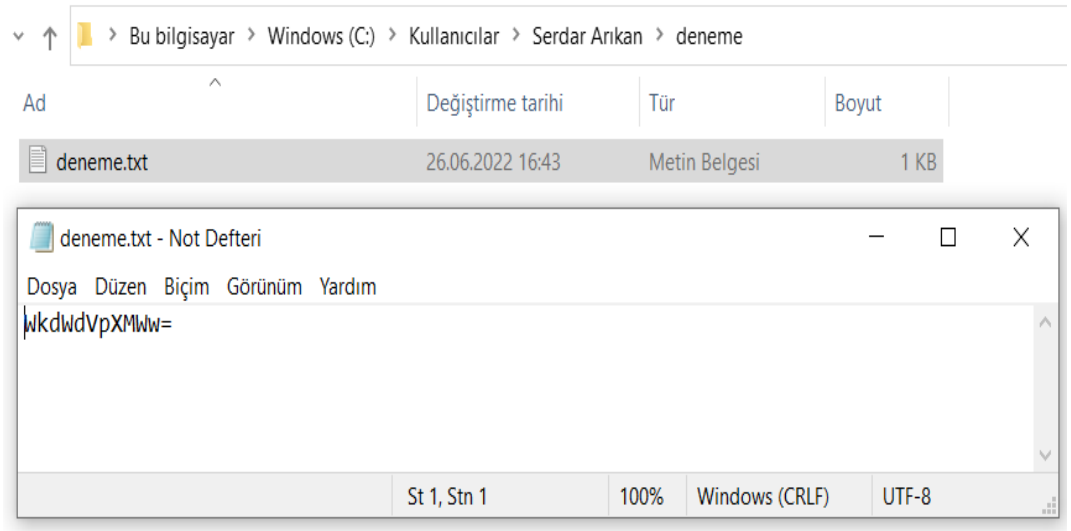
7.4. Uygulamanın Çalışma Adımları

Uygulama hazır bir .exe dosyasının çalıştırılmasıyla işlem yapmaktadır. Dosya çalıştırıldığında .py dosyasının 6.satırında işaret edilen dizindeki tüm belgeleri .txt (metin belgesi) formatına çevirip daha sonra base64 algoritması ile şifreliyor.

Uygulama çalıştırılmadan önceki hali Şekil 7.2'deki gibidir. Çalıştırıldıkan sonraki hali ise Şekil 7.3'de görüldüğü gibidir.



Şekil 7.2 .exe dosyası çalıştırılmadan önce dosyaların hali



Şekil 7.3 .exe dosyası çalıştırıldıktan önce dosyaların hali

8. Sonuç

Bu çalışmada casus ve zararlı yazılımların bulaşma teknikleri, belirtileri, türleri ve bu yazılımlardan korunma teknikleri incelenmiştir. Bunun yanı sıra literatürde bulunan çalışmalar da incelenerek araştırılması tavsiye edilen kaynaklar önerilmiştir. Çalışmanın insanları bilgi ve bilgi güvenliği hakkında ve kendi kişisel verilerini daha dikkatli bir şekilde korumaları hakkında onları bilinçlendirmesi amaçlanmıştır.

Bilgisayarınızı internete bağladığınız andan itibaren bu tür yazılımlara açık hale geldiğini unutmamalı ve buna uygun hareket etmelisiniz. Bilgisayarınızda mutlaka ücretli veya ücretsiz güvenilir antivirüs ve anticasus yazılımlar bulunmalıdır. Güvenlik yazılımları yeni casus ve zararlı yazılımlara karşı kendilerini sürekli olarak güncellemektedir bu yüzden sizde kullandığınız yazılımı sürekli güncelleyerek güvenliğinizi arttırmalısınız. Aynı şekilde işletim sistemi üreticileri de kendilerini casus ve zararlı yazılımlara karşı güncellemekte ve kullanıcılar tarafından güncellemelerin yapılmasını önermektedir.

Çalışmanın içeriğinden de malum olduğu üzere casus ve zararlı yazılım üreticisi bilgisayar korsanları sürekli kendilerini geliştirerek varolan türleri güçlendirmeye ve yeni türler ortaya çıkarmaya devam etmektedir. Bu tür yazılımlardan korunmak isteyen kullanıcıların sürekli olarak sistemlerini kontrol etmeleri gerekmektedir. Bu kontrol işlemi sadece güvenlik yazılımlarına bırakılmamalı ve etkileşimde bulunan tm bilgisayar ve dosyalara şüpheyle yaklaşımalıdır. Özellikle tanınmayan kaynaklardan gelen e-postaların eklerinin ve bağlantılarının kullanılmaması önem arz etmektedir.

Kaynaklar

[1] 50 years of malware? not really. 50 years of computer worms? that's a different story... - SANS internet storm center,.

[2] Adware - wikipedia, https://en.wikipedia.org/wiki/adware.

[3] ARPANET - wikipedia, https://en.wikipedia.org/wiki/arpanet.

[4] Bilgi güvenliği.

[5] Bilgisayar virüsü - vikipedi.

[6] Bilgisayar virüsü veya bilgisayar solucanı nedir?, https://www.kaspersky.com.tr/resource-center/threats/viruses-worms.

[7] Browser hijacker nedir? sisteme bulaştığında nasıl temizlenir? - blog | berqnet, https://berqnet.com/blog/browser-hijacker.

[8] Computer worm - wikipedia.

[9] Data - wikipedia, https://en.wikipedia.org/wiki/data.

[10] Fidye yazılımı nedir? | fidye yazılımlarından korunma | kaspersky, https://www.kaspersky.com.tr/resource-center/threats/ransomware.

[11] Keystroke logging - wikipedia.

[12] List of spyware programs - wikipedia.

[13] Phishing (oltalama) saldırısı nedir? - berqnet, https://berqnet.com/blog/phishing-oltalama-saldirisi-nedir.

[14] Phishing (oltalama) saldırısı nedir? nasıl Önlenir?, https://www.ekonomist.com.tr/encyclopedia/phishing-oltalama-saldirisi-nedir-nasil-onlenir.

[15] Phishing (yemleme-oltalama) yöntemi - bilgi İşlem daire başkanlığı | eskişehir osmangazi Üniversitesi, https://bidb.ogu.edu.tr/duyuru/detay/27/phishing-yemleme-oltalama-yontemi.

[16] Ransomware - wikipedia, https://en.wikipedia.org/wiki/ransomware.

[17] Ransomware back in big way, 181.5 million attacks since january - help net security, https://www.helpnetsecurity.com/2018/07/11/2018-sonicwall-cyber-threat-report/.

[18] Reklam yazılımı | İnternet güvenliği tehditleri, https://www.kaspersky.com.tr/resource-center/threats/adware.

[19] Solucan (virüs) - vikipedi.

[20] Spyware - wikipedia, https://en.wikipedia.org/wiki/spyware.

[21] The spyware inferno - CNET news, https://web.archive.org/web/20110510085748/http://news.cnet.com/2010-1032-5307831.html.

[22] Truva atı (bilgisayar) - vikipedi.

[23] Truva atı nedir, korunma ve kaldırma yolları nelerdir | ESET | ESET, https://www.eset.com/tr/trojan-horse/.

[24] WannaCry - vikipedi, https://tr.wikipedia.org/wiki/wannacry.

[25] What is browser hijacking? how to get rid of it?, https://www.kaspersky.com/resource-center/threats/browser-hijacking.

[26] Alper Aytekin, Ahmet Ayaz, and Fatma Tüminçin Eda Bektaş. Mobil cihazları etkileyen zararlı yazılımlar ve korunma yöntemleri. pages 244–252.

[27] İbrahim Alper Doğru Anıl Utku. Android kötücül yazılımlar için izin tabanlı tespit sistemi. 32(4):1015–1024.

[28] Soner Çelik Barış Çeliktaş. Güncel siber güvenlik tehditleri : Fidye yazılımlar. 3(5):105–132.

[29] Christopher Sean Cordes. Monsters in the closet: Spyware awareness and prevention. 28(2):53–56.

[30] Elif Ekiz and Şerif Bahtiyar. Zararlı yazılımların farklı İşletim sistemlerine etkileri.

[31] Gürol Canbek and Şeref Sağıroğlu. *Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri*.

[32] Şeref Sağıroğlu Gürol Canbek. Casus yazılımlar: Bulaşma yöntemleri ve Önlemler. 23(1):165–180.

[33] Şeref Sağıroğlu Gürol Canbek. Kötücül ve casus yazılımlar: Kapsamlı bir araştırma. 22(1):121–136.

[34] Michael Miller. *PC Güvenliği ve Bilgisayar Virüsleri (Absolute PC Security and Privacy)*. ALFA Kitap.

[35] Şahin Kara Resul Daş and M. Zekeriya Gündüz. Casus yazılımların bilgisayar sistemlerine bulaşma belirtileri ve Çözüm Önerileri.

[36] Metin Kesler Semih Çakır. Bilgisayar güvenliğini tehdit eden virüsler ve antivirüs yazılımları.

[37] Uğur Çelişken. *10 Adımda Bilgisayar Güvenliği*. Kodlab.

[38] İlker Kara. Truva atı zararlı yazılımlarının tespit, teknik analiz ve Çözüm Önerileri. 1.

[39] İlker Kara. Web tabanlı zararlı yazılımların saldırı yöntemleri ve analiz teknikleri. 5:46–53.

[40] Şeref Sağıroğlu and Gürol Canbek. Bilgisayar sistemlerine yapılan saldırılar ve türleri. 23:1–12.