Gazi Üniv. Müh. Mim. Fak. Der.
Cilt 23, No 1, 165-180, 2008

J. Fac. Eng. Arch. Gazi Univ.
Vol 23, No 1, 165-180, 2008

CASUS YAZILIMLAR: BULAŞMA YÖNTEMLERİ VE ÖNLEMLER

Gürol CANBEK ve Şeref SAĞIROĞLU
Bilgisayar Mühendisliği Bölümü, Mühendislik-Mimarlık Fakültesi, Gazi Üniversitesi, Maltepe, 06570, Ankara
gurol44@gmail.com, ss@gazi.edu.tr

(Geliş/Received: 21.03.2007; Kabul/Accepted: 17.09.2007)

ÖZET

Casus yazılımlar, bilgi ve bilgisayar güvenliğinde en önemli ve gittikçe yaygınlaşan tehdit ve saldırıların başında gelmektedir. Bu yazılımların kötü niyetli kullanımı sonucunda, bilişim teknolojilerinden yararlanmak isteyen her türlü kullanıcı ve kurum oldukça ciddi zararlara maruz kalmaktadır. Bu çalışmada, casus yazılımların bilgisayar sistemlerine bulaşabilmek için sık bir şekilde kullandıkları yöntemler incelenmiştir. Bu yöntemler oldukça somut örneklerle desteklenmiştir. Casus yazılımlara karşı kullanıcı ve sistem yöneticisi seviyesinde alınabilecek önlemler, bir araya getirilerek sunulmuştur. Casus yazılımların bulaşma tekniklerinin farkında olunması, bu yazılımlara karşı uyanık olunmasını sağlayacak; belirtilen önlemlerin takip edilip uygulanması etkin bir korunma sağlayacaktır.

Anahtar Kelimeler: Casus yazılım, bilgisayar güvenliği, bulaşma ve korunma yöntemleri.

SPYWARE: INFECTION METHODS AND PREVENTIVE MEASURES

ABSTRACT

Spyware is one of the top threats and attacks becoming widespread and dangerous in information and computer security. As a result of malicious usage of spyware, all sort of home and corporative users trying to make use of computer technologies are exposed to severe losses. We review the methods that spyware uses to infect computer systems. The methods are supported by concrete examples. The preventive measures against spyware are presented in both user and system administrator level. Comprehending spyware infection methods makes users wide-awake and following and applying the measures presented ensures the effective protection.

Keywords: Spyware, computer security, infection, prevention.

1. GİRİŞ (INTRODUCTION)

Bilişim teknolojilerinin yoğun bir şekilde kullanılması sonucunda; bu ortamdan bilgisayar ve İnternet aracılığıyla yararlanmak isteyen kullanıcılar, bilgi ve bilgisayar güvenliği açısından çok çeşitli saldırı ve tehditlere maruz kalmaktadır [1]. Virüsler, solucanlar, Truva atları, arka kapılar, mesaj sağanakları, kök kullanıcı takımları, telefon çeviriciler, korunmasızlık sömürücüleri, klavye dinleme sistemleri, tarayıcı soyma ve casus yazılımlar gibi genel kötücül yazılımlar dışında; çok çeşitli değişik kötücül yazılımlar artan sayı ve çeşitlilikte kullanıcı ve kurumları değişik boyutlarda zarara uğratmaktadır [2]. Özellikle ev kullanıcıları ve çocukların bilinçsiz ve bilgisiz olmaları, bu tür kötü niyetli yazılımların bilgisayar sistemlerine sızmasına, bulaşmasına, sisteme ve kullanıcıya zarar vermesini kolaylaştırmaktadır.

Casus yazılımların bilişim suçları kapsamında da kullanılması sonucunda sebep olduğu zararlar da gün geçtikçe artmaktadır [3]. Amerika'da FBI tarafından 2005 yılında 2000'den fazla şirket içinde yapılan bir araştırmada, bu şirketlerin %64'ünün casus yazılım ve bilgisayarla ilişkili suçlardan mali zararlara maruz kaldığı belirlenmiştir. FBI oluşan bu zararın yaklaşık 62 milyar ABD doları olduğunu tahmin etmektedir. Webroot, 2005 yılı boyunca 400 binden fazla sitede casus yazılım tespit etmiştir [4]. Bu güvenlik firmasının 2005 yılında Amerika'da 228 şirkette gerçekleştirdiği araştırmada, casus yazılımların firmalarda yol açtığı zararların neler olduğu Çizelge 1'de gösterilmektedir.

Çizelge 1. Casus yazılımların şirketlerde yol açtığı zararlar, 2005 [4] (The effects that spyware caused in organizations, 2005)

Casus Yazılımın Sebep Olduğu Etki	Yüzde
Sistem başarımını düşürme	% 61
Sistem bozuk kalma süresinde (down time) artış	% 43
Çalışanların üretkenliğini düşürme	% 33
Yardım masası çağrılarında artış	% 24
Ücretlilerin kendi maaşlarında kayıp	% 11
Gizli bilgilerin ele geçirilmesi	% 11
İş verilerinin tekrar kurtarılmasına sebep olma	% 11
Diğer	% 11

Casus yazılımların bu kadar etkin ve yaygın olması, bu konuda yapılması gerekenlerin ve alınması gerekli olan önlemlerin belirlenmesi ve uygulanmasındaki zorunluluğu ve aciliyeti göstermektedir. Bu çalışmada, bilgisayar sistemlerine sızma ve yazılımlara bulaşma yöntemleri ile alınacak koruyucu önlemler ayrıntılı olarak incelenmektedir. Sunulan bu çalışmada, alınması gereken önlemlerin dikkatlice takip edilmesi ve uygulanması ile kullanıcılar, casus yazılımlara karşı önemli bir korunma sağlayacaktır.

Bu çalışmada, Bölüm 2'de öncelikle kullanıcıların kendi sistemlerinde casus yazılım olup olmadığını gösteren belirtilerin neler olabileceği sunulmuştur. Bölüm 3'de casus yazılımların sistemlere bulaşmak için ne gibi yöntemler uyguladığı oldukça ilginç örneklerle aktarılmaktadır. Bölüm 4'de özellikle yasal açıdan yazılım kurulumunda gerekli olan; fakat casus yazılımlar tarafından çoğu zaman kötüye kullanılan uç kullanıcı lisans sözleşmeleri (EULA) irdelenmiştir. Bölüm 5'de yine casus yazılımlar tarafından İnternet üzerinde sıklıkla başvurulan kaçak indirme yöntemi ele alınmıştır. Bölüm 6'da sistemlere meşru bir yazılım görüntüsünde kurulmuş casus yazılımların, kendilerini sistemden kaldırmak isteyen kullanıcılara nasıl güçlük çıkardıkları ve kaldırım mekanizmalarında kullandıkları sıra dışı numaralar özetlenmiştir. Bölüm 7'de, literatürden ve yazarların deneyimlerinden, casus yazılımlara karşı kullanıcı ve sistem yöneticisi seviyesinde alınabilecek önlemler bir araya getirilmiş ve maddeler halinde sunulmuştur. Bu önlemlerin kullanıcılar tarafından sıkı bir şekilde takip edilmesi ve uygulanması; casus yazılımların sistemlere bulaşmasını önleyecek, sistemlere, bilgilere, bilgisayarlara ve yazılımlara verecekleri zararlar azaltılabilecektir. Bölüm 8'de ise bu çalışmadan elde edilen sonuçlar değerlendirilmiştir.

2. CASUS YAZILIM BELİRTİLERİ (SYMPTOMS OF SPYWARE)

Casus yazılımlar, bir bilgisayar sistemine bulaştıktan sonra işlerini gizlice yapmaya çalışıp; ulaşacakları amaca sessizce erişmek isterler. Fakat çoğu kez, casus yazılım tanısını koymada bazı önemli ve yaygın belirtiler, biraz dikkatli olunduğunda oldukça kayda değer deliller sunmaktadır. Eğer,

- Bilgisayarınızın her zamanki başarımı düşüyorsa ya da kısa süreli olarak durduk yere bilgisayarınız yavaşlamaya başlamışsa,
- İnternet üzerinde tarayıcınızla sörf ederken istemediğiniz siteler karşınıza çıkıyorsa,
- İnternet tarayıcınızdaki arama çubuğu bölümünde aramak istediğiniz anahtar kelimeyi girdiğinizde normalde kullanmak üzere ayarladığınız arama motoru yerine başka bir arama motoru arama sonuçlarını gösteriyorsa,
- İnternet tarayıcınızdaki Sık Kullanılanlar veya Yer İmi bölümünde sizin eklemediğiniz yabancı sitelere bağlantılar eklenmişse,
- İnternet tarayıcınızın başlangıçta gösterdiği site olan "Başlangıç Sayfanız", sizin ayarladığınızdan başka bir siteyi gösteriyorsa ve bu ayarı tekrar değiştirseniz de yine ayarladığınızdan farklı siteler açılışta ortaya çıkıyorsa,
- İnternet tarayıcınızda daha önce görmediğiniz araç çubukları varsa,
- Sistem tepsinizde daha önce görmediğiniz bir program simgesi varsa,
- İnternet'e bağlantınız olmadığı durumlarda bile size adınızla hitap eden çıkıveren reklâmlar görüyorsanız,
- İnternet sayfanızda bazı tuşlar (örneğin bir web formu doldururken bir sonraki yazım alanına geçmek için kullandığınız sekme tuşu) çalışmıyorsa,
- Bilgisayarınızla faal olarak çalışmadığınız bir sırada bilgisayar kasanızdaki sabit disk hareketini gösteren lamba sürekli yanıp sönüyorsa,
- 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,
- İnternet'e modem ile bağlanıp da büyük meblağlarda telefon faturası aldıysanız

sisteminizde çok büyük ihtimalle casus yazılım bulunmaktadır [5]. Sistemine bir casus yazılımın bulaştığını bu tür bulgular sonucunda farkına varan bir kullanıcının aklına gelen ilk soru "Acaba bu yazılım sistemime nasıl bulaştı?" olacaktır. Bu yerinde sorunun cevabı, takip eden kısımda örneklerle verilmeye çalışılmıştır.

3. BULAŞMA TEKNİKLERİ (INFECTION METHODS)

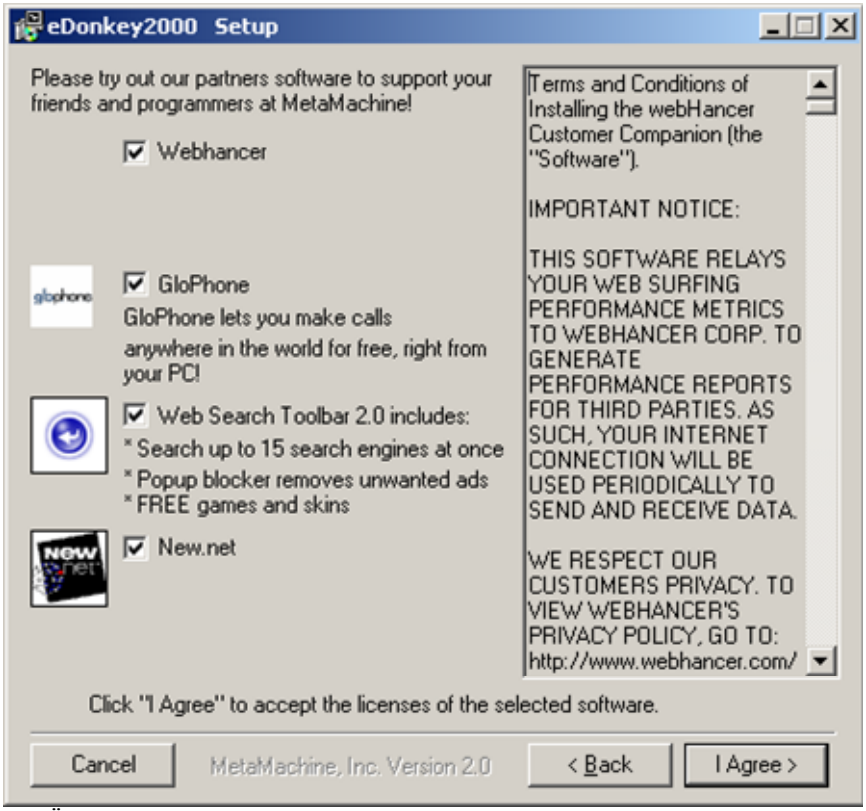
Casus yazılımların bir bilgisayar sistemine bulaşması çoğunlukla basit sayılabilecek yaklaşımlar kullanılarak çeşitli şekillerde olabilmektedir. Casus yazılımların yayılması ile ilgili birçok teknik, bu bölümde örneklerle anlatılacaktır. Genel olarak

bakıldığında bu tür kötücül yazılımların dağıtılmasında kullanılabilecek yöntemler;

- İşletim sistemlerinde casus yazılım, arka kapı gibi yapıların bulunma olasılığı,
- Farklı üreticilerden aldıkları parçaları bir araya getirerek bilgisayar yapan firmalar olarak tanımlanan özgün donatım üreticilerinin (OEM), bilgisayarlarını müşterilerine satmadan önce kurdukları yazılımlar arasında kasten veya bilmeden casus yazılım bulunması,
- Çoğunlukla ücretsiz dağıtılan uçtan uça dosya paylaşımı (P2P) programları, ekran koruyucular ve oyunlar içine casus yazılım bohçalanması ile bulaşma,
- Faydalı bir yazılım kurulumunun yanında; dosya, klasör ve sistem kütüğü isimlerini zararsız, bilindik veya sisteme ait isimler vererek saptanmasını ve sistemden kaldırılmasını zorlaştırarak sisteme yerleşme,
- Kök kullanıcı takımları (rootkit) yardımıyla sistemde kendi giriş (login), proses ve dosyalarını tamamen saklayarak sistemde çalışma,
- Herhangi bir programın kurulumu sırasında, aslında casus yazılım özelliği taşıyan başka yardımcı ve ek yazılımların kullanıcıya belirtilerek kurdurulması,
- E-posta dosya eklentisi ile e-posta'da verilen bir web adresine gidildiğinde veya doğrudan HTML içerikli e-postaların okunması ile casus yazılım bulaşması,
- İnternet tarayıcılarında bulunan korunmasızlık ve açıklardan yararlanarak kurulum,
- Özellikle İnternet üzerinden kullanıcıya aldatıcı mesajlarla yanıltıp; her hangi bir casus yazılımın kurulumunun başlatılması,
- Uç kullanıcı lisans sözleşmelerinde yanıltıcı veya eksik bildirim ile kullanıcıya zararlı bir yazılımı bilgisayarına kurdurtma,
- Çocukların ve bilinçsiz kullanıcıları aldatıcı taktikler kullanmak,
- Çok çeşitli sosyal mühendislik ve insan hatası yöntemleri

olarak özetlenebilir [1, 4, 6].

Casus yazılımlar bilgisayarlara bulaşmak ve yayılmak için, İnternet üzerinde, pek de dürüst olmayan birçok teknik kullanmaktadırlar. Genelde, oldukça faydalı ve işe yarayacak gibi gösterilmeye çalışan ve "bedava" olduğu sürekli vurgulanan programlar, kullanıcılara çeşitli şekilde önerilmektedir. Bazı teknikler, çok dikkat çekmeden kullanıcıların bilinçaltını bile etkileyebilmektedir. Faydalı olabileceğini düşünen, üstelik de bedava olan bu yazılımları kendi bilgisayarlarına kuranların, karşılaşabileceği tehlikelerin boyutlarının neler olabileceğini kestirmek zordur.



Şekil 1. Örnek bir dosya paylaşım programı kurulumunda ilave program kurulumları
(Installing additional programs in file sharing software setup)

Şekil 2. Casus yazılımların çıkıveren reklâmlarına örnekler (Examples from pop-up ads of spyware)

Dahası, aslında casus yazılım olan bir programı kurmaya ikna olan veya ikna edilen kişiye, bir de o programla beraber başka casus yazılımlar kurdurma yoluna da gidilerek; daha çok casus yazılım bir birleri ile işbirliği içinde sistemlere sızabilmektedir. Şekil 1'de bunu gösteren çok tipik bir örnek verilmiştir. Burada bir şekilde eDonkey2000 adında bir dosya paylaşım programını sistemine kurmayı düşünen kişiye, kurulum sırasında dört adet başka programın kurulması, onay kutuları da kullanıcının zahmet etmesini önlemek amacıyla varsayılan olarak seçili olacak şekilde sunulmaktadır. "Bir taşla dört kuş vurmak" şeklinde özetlenebilecek bu yöntem, bu sıralar hemen hemen bütün casus yazılımların kurulum safhasında karşımıza çıkmaktadır.

Bu tür casus yazılımlar, herhangi bir bilgisayara kurulduktan sonra, kendi temel amacı dışında işlev görmeye başlamaktadır. Öyle ki, kullanıcının gezdiği sitelerin HTML kodlarının asıllarını bile kullanıcının haberi olmadan, dinamik olarak değiştirip, anlaşmış oldukları kendi firmaların reklâmlarını bile vermeye cüret etmektedir.

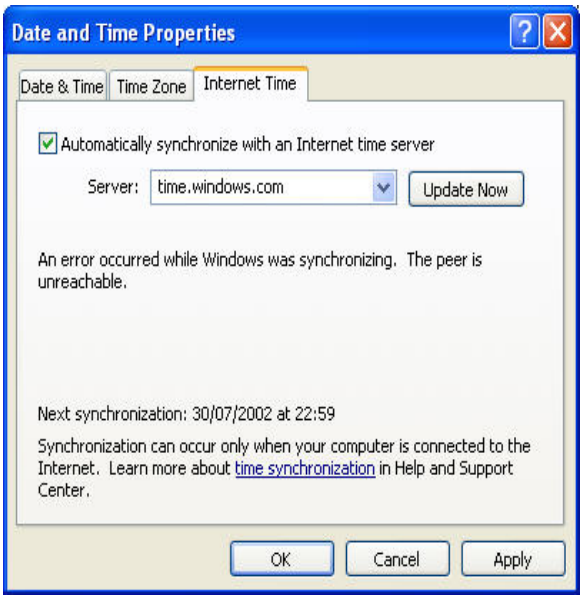
HTML kodu değişen sayfada Şekil 2'de görüldüğü gibi birçok şey vaat eden, çeşitli reklâmlarla kullanıcılar kandırılmaya ve reklâmda sunulan ürünleri almaya özendirilebilmektedir.

Sunulan reklâmlar; kumar, bahis, faiz karşılığında ödünç para verme, seyahat (uçak biletleri, oteller, araç kiralama, deniz gezisi), kredi kartları, elektronik ve haberleşme, cinsel sağlık, sigorta, çöpçatanlık, sağlık ve ilaçlar (diyet, vitaminler, saç onarımı, kalp krizi önleme), müzik, kitaplar ve filmler (kitap kulüpleri, CD kulüpleri, DVD kiralama, bilet temini), bankacılık ve yatırım, ev ve ev ürünleri, giysi ve aksesuarlar, eğitim (çevrimiçi derece alma, uzaktan eğitim, diploma alma, tatil eğitimi), çiçekler, yazıcı sarf malzemeleri, açık artırma ve sigara gibi birçok konuda olabilmektedir. Görüldüğü gibi her bir konu, çok sayıda insanı cezp edecek türdendir.

Casus yazılımların, sisteme sızabilmek için kullandığı ve aslında oldukça "zavallı" olarak nitelendirilebilecek bir başka taktik de; sahte pencere veya diyaloglar kullanmaktır. Kullanıcılar, İnternet sayfalarında gezinirken İnternet tarayıcısına ait çıkıveren pencerelere karşı az da olsa daha çekimserdirler. Bu tür pencereler, kullanıcılar tarafından görülür görülmez, genelde içeriğine bakılmadan hemen kapatılırlar. İşletim sisteminden gelen mesaj ve diyalog kutuların ise kullanıcılar tarafından daha önemsendiği düşünülmektedir. Bu gerçekten hareket eden casus yazılımlar, İnternet sitelerinde standart işletim sistemi diyalog kutularına benzeyen mesajlar göstermektedirler.

Şekil 3'de bir örneğinin görülebileceği gibi, bir sitede geniş bir alanda bilgisayarınızın sistem saatinin tam olarak doğru olmadığını gösteren bir ileti, sanki bir sistem mesajı gibi gösterilmektedir. Aslında resim olan bu mesaj, değişik şekillerde gezilen diğer sayfalarda gösterilerek kullanıcının dikkati çekilmek istenir. Kullanıcı, bu resme tıkladığında (OK düğmesine basıp basmadığının bir önemi de yoktur) önerilen saat düzeltici programını, indireceğini düşünebilir; fakat aslında bu diğer casus yazılımların kurulabilmesi için geliştirilmiş ve aslında oldukça bayağı olan bir yemdir.

Sistem saatinin doğruluğu konusunda biraz daha dikkatli olunursa; aslında Microsoft, Windows XP ile kullanıcılarının doğru ve hassas sistem saatine sahip olmaları için otomatik saat senkronizasyonu özelliğini işletim sistemine bütünleştirmiştir. Şekil 4'de görüldüğü gibi, kullanıcılar bu özelliği etkinleştirerek saatlerini hiç bir harici programa ihtiyaç duymadan doğrulatabilirler.



Şekil 3. Windows XP ile birlikte gelen otomatik saat senkronizasyonu penceresi (Automatic time synchronization of Windows XP)

Normalde bir web sunucusuna ait bir siteye bağlanan kişinin hangi işletim sistemini kullandığı, sunucu tarafında çok kolay bir şekilde algılanılabilmektedir. Dolayısıyla Windows XP yüklü bir bilgisayar için böyle bir sayfada sunucunun "saatiniz yanlış olabilir" diye bir mesajı göstermesi, art niyet dışında hiç bir şeyle ifade edilemez. Fakat casus yazılımların böyle gereksiz programlarla sistemlere bulaşabilmesi için kötü niyetli web sitelerinde, hiç ayırt etmeden kullanıcıların hepsine böyle bir mesaj verilebilmektedir.

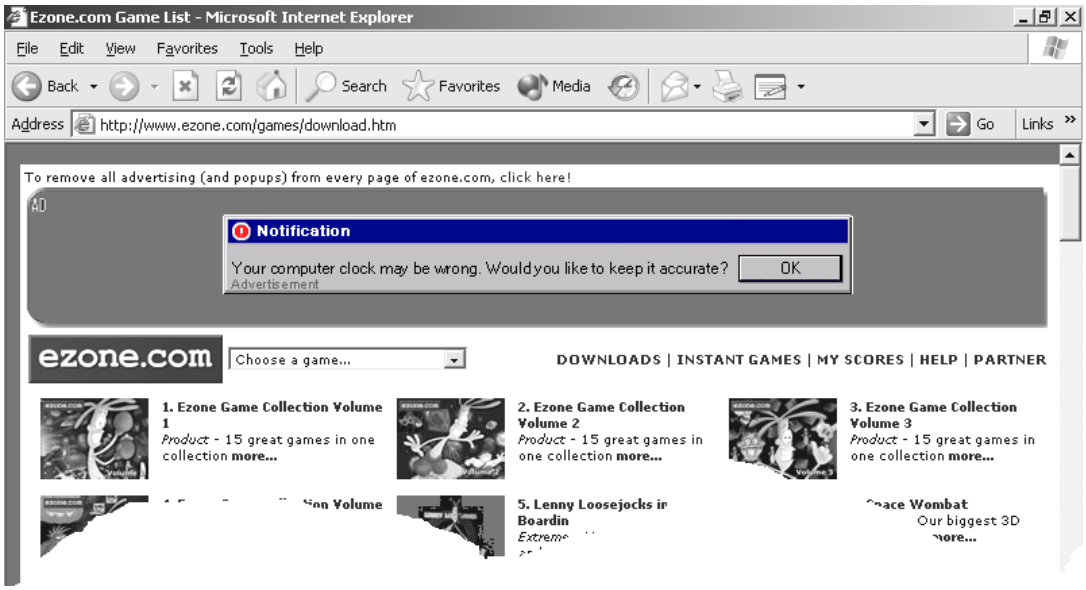
Bir başka ciddi konu da İnternet sitelerinden casus programın kurulabilmesini sağlamak için çocukların suiistimal edilmesidir.

Şekil 5'de gösterilen sayfada, çocukları özendirici bir tarz göze çarpmaktadır. Çocukların hoşuna gidecek çizgi kahraman, resim ve canlandırmalarla; oyun v.s. gibi yazılımlar içinde casus yazılımlar bilgisayara kopyalanabilmektedir. Bu tür sitelerden program indiren çocuklara, EULA'nın (Uç Kullanıcı Lisans Anlaşması) gösterilmesi de bir şey ifade etmez. Çünkü erişkinler gibi çocuklar da bu tür yazıları hiç okumaz ya da okusalar da anlamaları güçtür. Ebeveynlerin bu konuda dikkatli olmaları ve gerekli tedbirleri almaları gerekmektedir. Çocukların, bilgisayar ve İnternet üzerinden casus yazılımlarla kandırılmaları ve güvenliklerinin tehdit edilmesi mümkündür [7].

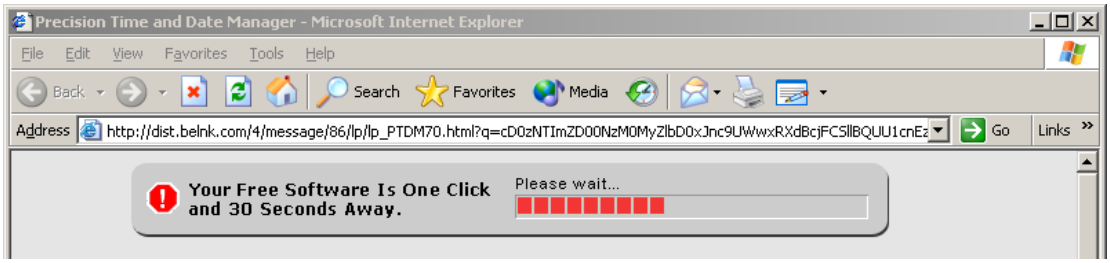
Bazı İnternet sitelerine erişimi veya bu sitelerden yazılım kurulumunu engelleyen WebSense gibi İnternet filtreleme yazılımları, bu tür adresleri engelleyebilmektedir. Fakat casus yazılım üreticileri, programlarını yeni satın aldıkları rasgele isimler içeren bir bölgeye taşıyarak, bu tür casussavar yazılımlardan bir süreliğine de olsa kaçabilmektedirler. Şekil 6'da görülebileceği gibi mesela "ezone.com" sitesi, saat senkronizasyonu yaptığını iddia eden yazılımın dağıtımını "dist.belnk.com/..." gibi "ezone.com" ile hiç alakası olmayan bir adresten yapmaktadır.

4. UÇ KULLANICI LİSANS ANLAŞMASI (EULA) (END-USER LICENSE AGREEMENT)

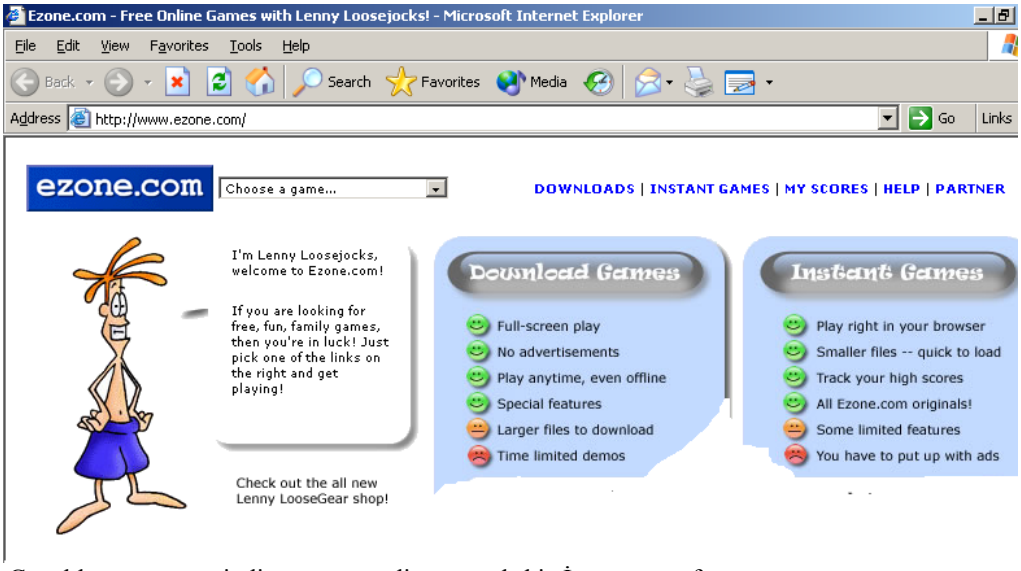
Programların kurulması sırasında normalde birçok kurulum programı veya sihirbazı, İngilizce EULA adı verilen bir anlaşma ile başlamaktadır. Anlaşma okunduktan sonra "Kabul ediyorum" ("I agree") düğmesine tıklanarak kurulum başlatılır. Bu durumda, anlaşmada belirtilen her şeyin kullanıcı tarafından kabul edildiği anlamı çıkmaktadır. Diğer durumda program kurulamaz. Ülkemiz için lisans anlaşması ile ilgili bir başka olumsuzluk, bu metinlerin genelde



Şekil 4. Sahte diyalog kutuları (fake dialog boxes)



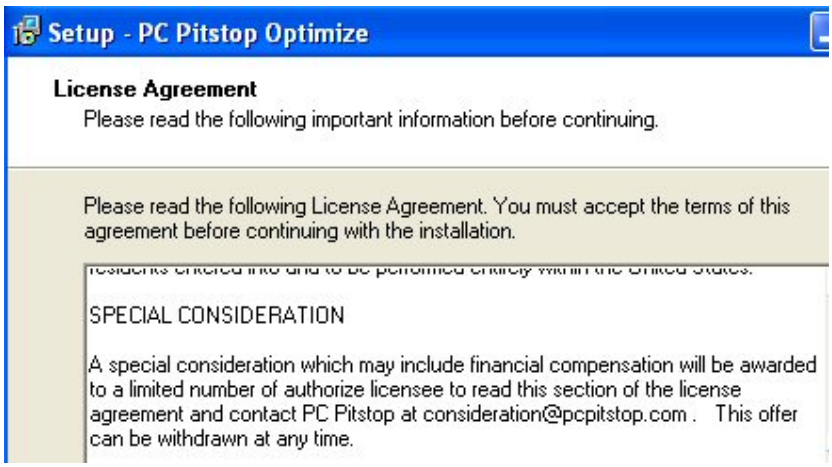
Şekil 5. Ana bölge adresinden farklı adres kullanarak casus yazılım dağıtımı (Spyware distribution using different address from main official domain address)



Şekil 6. Çocukları program indirmeye özendiren örnek bir İnternet sayfası(Sample web page encouraging children to download programs)

İngilizce olmasıdır. İngilizce bilmeyen veya yeterli seviyede bilmeyen kişiler, bu anlaşmaları anlamadan kabul etmek zorunda kalmaktadır.

Ne yazık ki lisans anlaşmasında yazılan metne, ya şöyle bir göz atılır ya da çoğunlukla yapıldığı gibi, hiç okunmadan anlaşma kabul edilir. Bunun böyle olduğu yaşanan bir olayla çok güzel bir şekilde gözler önüne serilmiştir. Bu olayda, casussavar yazılım ürünleri çıkaran bir firma, lisans anlaşmalarına gösterilen ilgisizliği gözler önüne sermek amacıyla, kendi casussavar yazılım lisans anlaşmasının içerisinde ve metnin ortalarında yer alan bir paragrafta, "bahse konu olan paragrafı okuyup; firmaya başvuranlara mali bir ödül vereceğini" beyan etmesine rağmen; 3000 adet program indirilmesinden sonra, ancak dört ay geçince bunu okuyan tek bir kişi çıkmış ve firmaya anlaşmada belirtilen e-posta adresinden başvurmuştur.



Şekil 7. Lisans anlaşmalarının okunmadığını göstermek amacıyla hazırlanan ödüllü bir uç kullanıcı lisans anlaşması [8] (Awarded EULA prepared for showing that users don't read EULAs)

Çizelge 2. Gizli bilgi toplama ve reklâm gösterme ile ilgili bilgi veren örnek bir EULA anlaşması
(Sample EULA informing about secret information gathering and advertisement)

"GAIN Publishing offers some of the most popular software available on the Internet free of charge ("GAIN-Supported Software") in exchange for your agreement to also install GAIN AdServer software ("GAIN"), which will display Pop-Up, Pop-Under, and other types of ads on your computer based on the information we collect as stated in this Privacy Statement. We refer to consumers who have GAIN on their system as 'Subscribers.'"	"GAIN Yayıncılık, bu Kişisel Gizlilik Bildirisinde ifade edildiği şekilde bilgisayarınızda topladığımız bilgilere dayanan Üste Çıkıveren, Altta Çıkıveren ve diğer türde reklâmlar gösteren, İnternet üzerinde var olan en popüler yazılımların bazılarını GAIN Reklam Sunucusu yazılımını da ("GAIN") ayrıca kurmak karşılığında ücretsiz olarak teklif eder. Sistemlerinde GAIN olan müşterilerden 'Aboneler' olarak bahsedilir."

Bu kişinin 3000$ ödül kazandığı firmanın İnternet sitesinde ifade edilmektedir [8]. Anlaşmanın örneği Şekil 7'de gösterilmektedir. Durumun vahametini gösteren bu örnek, birçok casus yazılımın aslında programın yapmakta olduğu kirli işleri lisans anlaşmalarında "çoğu kez" belirttikleri; fakat kullanıcıların bunları okumadan kabul etmeleri nedeniyle yasa önünde suçlu bulunmamalarının sağlandığının en güzel delilidir.

Anlaşmaları okumayı prensip haline getirseniz bile çeşitli güçlükler sizi beklemektedir. Casus yazılımlar, kurulumları sırasında bu tür anlaşmaların okunmasını bazı numaralarla daha da zor hale getirmektedirler. GAIN casus yazılımın 2004 Ekim sürümünün Uç Kullanıcı Lisans Anlaşması, 2550 kelimeden yani yedi sayfadan oluşmaktadır. Bu kadar bol metin içinde programın yaptığı işler, Çizelge 2'de görüldüğü gibi net bir şekilde anlatılmaktadır:
Bunun dışında birçok ilginç ifade bu tür anlaşmaların satır aralarında var olabilir. Çizelge 3'de görüldüğü gibi aynı anlaşmada, program kaldırılmasının, casussavar yazılımlarla bile mümkün olmadığı çok rahat bir şekilde belirtilmektedir.

Çizelge 4'de yine aynı program ile ilgili ilginç bir ifade, net bir şekilde lisans anlaşmasında bulunmaktadır. Buna göre, programın yüklü olduğu bilgisayar ile programın sunucusu arasında ne gibi bir haberleşmenin olduğunu bulmaya çalışmak ve bu şekilde programın kullanıcı hakkında topladığı bilgilerin gerçekte neler olduğunu öğrenmek bile önlenmek istenmektedir [9].

Kullanılan başka bir numara da anlaşmanın okunurluluğunu azaltmaktır. Şekil 8'de GAIN programının önceki ve sonraki sürümleri için kullanılan EULA'nın ekran görüntüsü gösterilmektedir. İkinci örnekte okunurluk azdır ve kullanıcı muhtemelen o bölümü okumadan atlayacaktır.

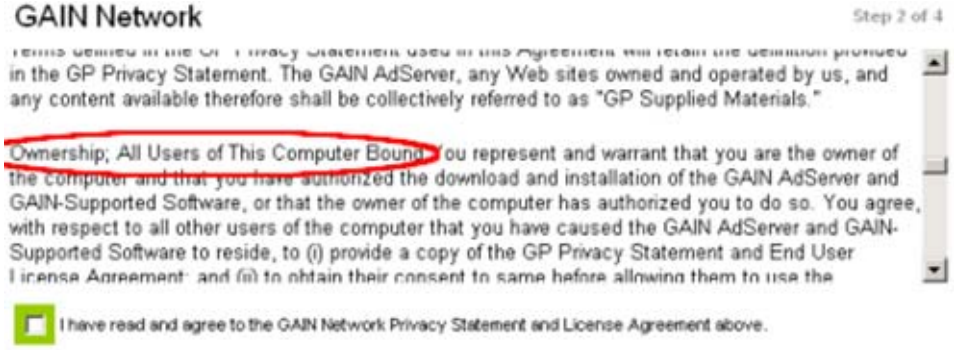
Çizelge 3. Casus yazılım anlaşmasında programın kaldırılmasının yasaklanması
(Prohibiting removal of program in spyware agreement)

"You agree that you will not use, or encourage others to use, any unauthorized means for the removal of the GAIN AdServer, or any GAIN-Supported Software from a computer."	"Bir bilgisayardan GAIN Reklâm Sunucusunun veya GAIN-Destekli herhangi bir yazılımın sistemden kaldırılması için hiç bir yetkisiz yöntem kullanmayacağınızı veya diğer kişileri buna teşvik etmeyeceğinizi kabul etmektesiniz."

Çizelge 4. Casus yazılımın anlaşmasında kendi topladığı ve gönderdiği bilgilerin incelenmesinin yasaklanması (Prohibiting to examine the information collected and transmitted by spyware)

"Any use of a packet sniffer or other device to intercept or access communications between GP and the GAIN AdServer is strictly prohibited."	"GP ve GAIN Reklâm Sunucusu arasındaki haberleşmeleri, araya girip kesmek veya bunlara erişmek için bir paket koklayıcı veya diğer tür cihazların herhangi şekilde kullanımı kesinlikle yasaktır."

(a) EULA'nın bölüm başlıkları koyu ve ayrı yazılmış önceki hali



(b) Bölüm başlığı normal şekilde yazılmış sonraki hali

Şekil 8. EULA'nın kullanıcı tarafından anlaşılmasının güçleştirilmesine bir örnek (Deliberate difficulties of reading EULA)

Şekil 9. Önceki sürümlerde yer alan "Printable Version" seçeneği (soldaki resim) sonraki sürümlerde kaldırılmış (sağdaki resim) (Removing "Printable Version" option in EULA window)

Bu tür programlarda çok uzun olan anlaşma metni, bir de daha düşük genişlikte bir kutuya yazılarak kullanıcının anlaşmayı okuma hevesinin kırılması istenmektedir. Kullanıcı arabirimi ile ilgili yapılan bir araştırmada, 10 ile 12cm arasında genişlikte pencerelere yazılan yazıların, en hızlı okumayı sağladığı belirtilmektedir [10]. Çoğu casus yazılımın kurulum programlarında, lisans anlaşması daha kısa genişlikte yazılarak daha çok kaydırmaya sebep olunup metnin okunma hızı düşürülmektedir. Şekil 1'de böyle bir kurulum ekranı gözükmektedir.

Çoğu kurulum ekranında, hem bütün anlaşmanın daha rahat okunabilmesi için hem de arşiv olarak saklanabilmesi için anlaşmanın yazıcı çıktısını alma seçeneği konulmaktadır. Kötücül yazılımların bir kısmında bu seçenek de kaldırılmıştır. Şekil 9'da görülebileceği gibi KaZaa programının ilk sürümlerinde yer alan Yazıcı Sürümü (Printable Version) seçeneği sonraki sürümlerinde "her nedense" gerek görülmeyerek kaldırılmıştır [9].

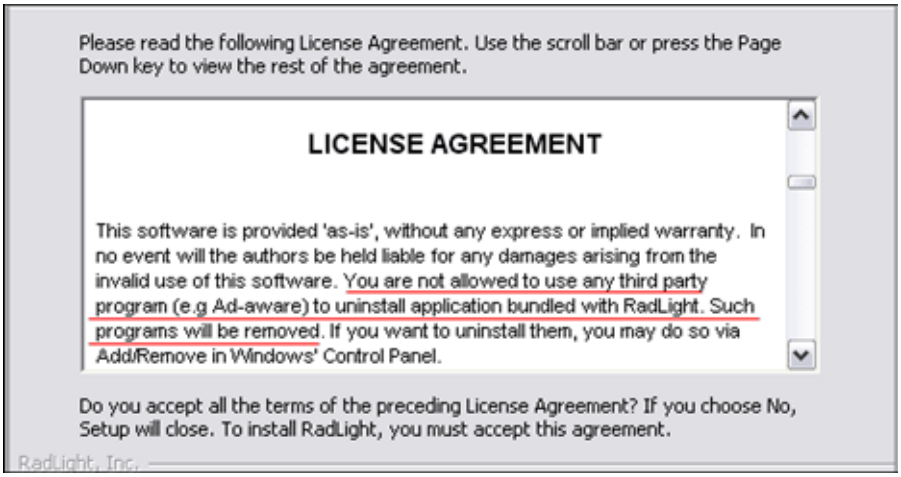
Bunun gibi birçok kandırmaca, kullanıcıları tuzağa düşürmek ve yıldırmak için yapılmaktadır. Bazı taktikler ise "bu kadarı da olmaz" dedirtecek türdendir. Mesela lisans anlaşmasının tamamını görmeye yarayan dikey kaydırma çubukları çalışmaz hale getirilmiş veya kaydırıldığında geride hiç bir şey bulunmayan kurulum programlarına bile rastlamak mümkündür.

Çizelge 5. P2P (Eşten Eşe) dosya paylaşım programlarının lisans anlaşmaları, kurdukları diğer yazılımlar ve sistem kütüğüne ve dosya sistemine ekledikleri öğelerin dökümü [11]
(Additional items installed in P2P file sharing programs and their EULAs)

P2P Dosya Paylaşım Programı	*Ana kurulum ekranında ifşa edilen gerekli kurulumlar*	*Ana kurulumda ifşa edilen seçimlik kurulumlar*	*Sadece lisans anlaşması içinde ifşa edilen kurulumlar*	*Bohçalanmış yazılım*		*Sistem kütüğü (registry) eklentileri*		*Dosya sistemi eklentileri*	
				İnternet gezintilerinin izini sürme	*Tarayıcı içinde veya çevresinde reklâm gösterme*	*Anahtarlar*	*Değerler*	*Klasörler*	*Dosyalar*
eDonkey		Webhancer, GloPhone, Web Search Toolbar, New.net		Evet	Evet	280	944	23	353
	7767 kelime, 90 ekran sayfası. Satır başına3–5 kelime gösteren dar lisans penceresi. Birden fazla lisans tek bir metin kutusuna birleştirilmiş.								
iMesh			AskJeeves (MySearch) araç çubuğu	Hayır		488	1589	30	214
	5493 kelime, 56 ekran sayfası. Bir web araç çubuğu kurmasına rağmen “toolbar” (araç çubuğu) kelimesi asla kullanılmıyor. Lisans anlaşmasında kırık bağlantılar.								
Kazaa	Cydoor, GAIN, Instafinder, My Search Toolbar	Skype	Masaüstü simge eklentisi ("Your Free Casino Chips!" ve "Play Poker Now!")	Evet	Evet	845	1477	112	638
	22606 kelime, 182 ekran sayfası. Çok az başvurulan birden fazla lisans gösterilmiyor. Birden fazla lisans tek bir metin kutusuna birleştirilmiş. Harici belgelere anonim başvuru yapan birden fazla atıf. Ayrık bölüm başlıkları ana metin gövdesiyle birleştirilmiş. İzin verilen kaldırma yöntemlerinde sınırlama.								
LimeWire	"ads" (reklâm) ve "nagware"			Hayır	Hayır	134	527	61	864
	Hiç lisans gösterilmiyor veya başvuru belirtilmiyor.								
Morpheus			DirectRevenue	Evet	Evet	85	312	15	384
	4492 kelime, 44 ekran sayfası. Lisans anlaşmasında kırık bağlantı. İzin verilen kaldırma yöntemlerinde sınırlama. Diğer programları kaldırma izninin manalı bir şekilde verilmesi. Toplanan belirli bilgilerin açığa vurulmasında ihmal.								

Çizelge 5’de görüldüğü gibi bir programın kuruluşunun altında birçok gizli faaliyet yatmaktadır: sayfalarca lisans anlaşması metni, gizlenen diğer “bonus” kurulumlar ve sisteme eklenen yüzlerce sistem kütüğü eklentileri (kütük anahtarları ve değerleri) ile dosya sistemini dolduran yüzlerce eklentiler (klasörler ve dosyalar). Bu kadar eklenti ve gizlenme çabalarının, sadece dosya paylaşımını gerçekleştirmek; sistem saatini doğru tutmak veya hava durumunu anlık öğrenmek v.s. amacıyla yapılıyor olduğunu düşünmek, fazla iyimserlik olacaktır.

Lisans anlaşmalarının okunmadığı zaman ortaya çıkabilecek ilginç ve tehlikeli durumlardan birine bir örnek de RadLight adında ortam yürütücü (Media Player) programı verilebilir. SaveNow ve NewDotNet adında iki kötücül yazılım ile bohçalanmış bu programın kurulumu sırasında Şekil 10’da gösterildiği gibi bu iki kötücül yazılımı temizleme listesinde tutan Ad-aware casus yazılım koruma programını eğer



Şekil 10. RadLight kullanıcı anlaşmasında gözden kaçabilecek bir madde
(An item that may be ignored in RadLight EULA)

sistemde bulursa kaldıracağını belirtmektedir [12]. Durumun açığa çıkması sonucu oldukça tartışma oluşturan bu yöntem, casus yazılımların sergileyebileceği saldırgan yaklaşımların nerelere varabileceğini göstermektedir. Kullanıcılar, sistemlerine kurdukları bütün programların lisans anlaşmalarını dikkatlice okumalı ve bu tür taktiklere karşı uyanık olmalıdır.

5. KAÇAK İNDİRME (DRIVE-BY DOWNLOAD)

Gator firması, 2002 yılında İnternet üzerinde "kaçak indirme ActiveX" sürücüsünü tanıttı. Normal yazılım kurulumu yanında kaçak indirme, alakası bulunmayan bir İnternet sitesinde gezinirken, istenmeyen bir yazılımın kullanıcıdan habersiz veya kullanıcıyı yanıltarak indirilip, kurulması işlemidir. Özellikle web sitelerinde gezinirken herhangi bir program site tarafından indirilip kurulması durumunda İnternet Gezgini gibi tarayıcılar çıkıveren bir pencerede bu durumu belirten bir güvenlik uyarısını göstermektedir. Güvenilir web siteleri dışında casus yazılım içeren sitelerde bu tip güvenlik uyarılarında kullanıcıları yanıltma yoluna gidebilmektedir. Şekil 11'de, bu tür bir pencere görülmektedir.

Şekil 11. Lisans anlaşmasını kısa bir paragraf ile belirtmekle yetinen örnek bir kaçak indirme çıkıveren penceresi (A drive-by download window example showing the EULA just in one paragraph)

(a) Örnek 1

(b) Örnek 2

Şekil 12. İndirme ile sürücü diyaloglarının kullanıcıya yanıltmaya yönelik kullanım örnekleri (Examples of drive-by downloads that attempting to cheat the users)

Bu pencerede bulunan "X'den gelen içeriğe her zaman güven" (Always trust content from X) seçeneği çok dikkat edilmesi gereken bir kısımdır. Bu seçecek onaylanırsa, bundan sonra o firmanın yayınladığı bütün yazılımlar sisteme kullanıcıdan izin alınmadan kurulabilmektedir.

Şekil 12'de görülebileceği gibi bu tür diyalog kutuları şablon halindedir. Şekil 12 (a)'da şirket adı yerine "Devam etmek için Evet'i tıklayın" (CLICK YES TO CONTINUE) konularak, kullanıcının fazla düşünmeden istenileni yapması sağlanmaya

Şekil 13. Casus yazılımların Başlat menüsünde program kaldırma kısa yolunun da bulunduğu özel bir program grubu oluşturmamasına bir örnek (Spyware usually don't include their uninstaller in menus)

çalışılmaktadır. Şekil 12 (b)'de kurulmak istenen ürünün adı, "Virüssüz. Evet"i tıkla" (VIRUS FREE. CLICK ON "YES") olarak belirtilmiş ve kullanıcı yanıltılmaya çalışılmıştır. Bazı sitelerde gösterilen diyaloglarda, Hayır düğmesi bile tıklansa kullanıcıya devam etmesi için Evet'i tıklaması gerektiği belirten bir mesaj, kullanıcı usanıp Evet'i tıklayana kadar sürekli olarak gösterilmektedir. Buradan çıkmanın tek yolu tarayıcıyı Görev Yöneticisini kullanarak sonlandırmaktır.

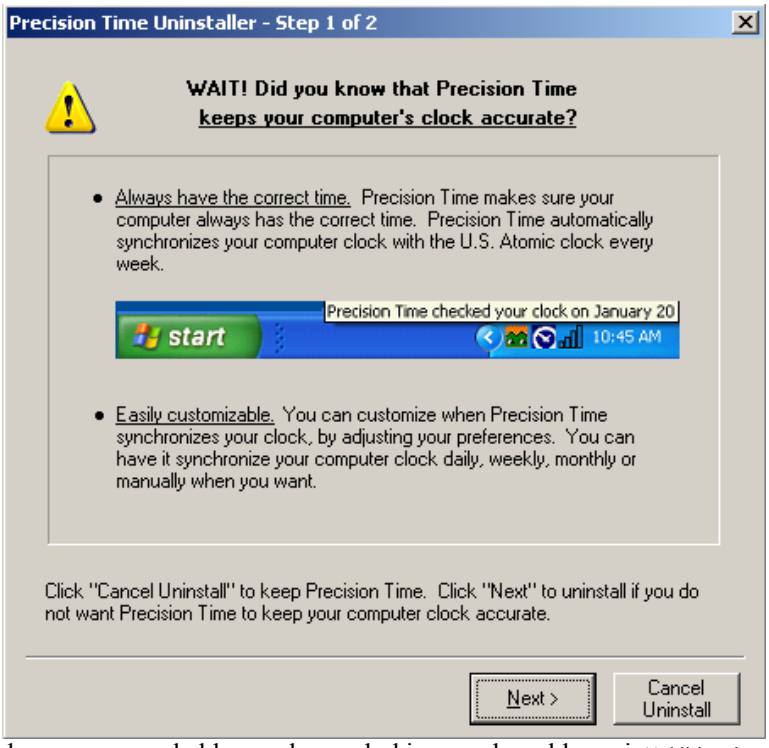
Güvenlik uyarılarının casus yazılım içeren bir siteden değil de güvenilir veya bilinen bir siteden göstermeye çalışan kaçak indirme saldırılarından biri de alttan çıkan kaçak indirme yöntemidir. Bu yöntemde kullanıcı sahte bir İnternet bağlantısını tıkladığında güvenilir bir sitenin içeriği gösterilir; fakat alt kısımda, örneğin bir HTML çerçevesinde çok küçük olarak diğer sitenin sayfası yüklenmiştir. Bu siteden kullanıcıya gösterilen güvenlik uyarısı, kullanıcının o an gezdiği sitenin adı ile gösterildiğinden; kullanıcı bu güvenlik uyarısını kabul edebilmektedir. Bu tür kaçak indirme yöntemlerine karşı kullanıcıların bilinçli ve uyanık olması gerekmektedir.

6. PROGRAM KALDIRMA MEKANİZMASI (UNINSTALL MECHANISM)

Bütün bu aşamalardan geçen bir casus yazılım, bir kere sisteme yerleştikten sonra, kendisini kurulduğu makineden atma ve silme çabalarına karşı da direnç göstermekte ve bunu yapmak isteyen kullanıcılara çeşitli zorluklar çıkarmaktadır. Kurulum sırasında oldukça yardım sever bir anlayış sergileyen casus yazılımlar, sıra programın kaldırılmasına gelince, oldukça "inatçı" bir tavır takınırlar. Yukarıda da bahsedildiği gibi, bu tür casus yazılımlar lisans anlaşmasında otomatik kaldırmayı bile yasaklayabilmektedirler.

Program kaldırmayı önlemek için kullanılan yöntemlerin en basiti olan ve hemen hemen her program ile beraber gelen standart "program kaldırma" rutinlerine sahip değildirler. Yani denetim masasındaki "Program Ekle/Kaldır" bölümünde kurulu bulunan programlar listesinde bulunmazlar. Casus yazılımlar çoğunlukla, Başlat (Start) menüsünde, Şekil 13'de gösterildiği gibi, program kaldırma menü seçeneğinin de bulunduğu bir grup olarak değil; sadece çalıştırılabilir dosyayı işaret eden kısa yollar halinde bulunur.

Şekil 14'de görüldüğü gibi Program Ekle/Kaldır bölümünde yazılımın kaldırılması olanağı tanındığı durumda ise program kaldırılmak istendiğinde, kullanıcıyı bir kez daha düşünmeye sevk eden, bir ara adım devreye girmektedir. Yufka yürekli deneyimsiz kullanıcılar buna kanıp programı kaldırmaktan vazgeçebilir.



Şekil 14. Casus yazılımın program kaldırma ekranında bir ara adım eklemesi (Additional step before uninstalling the spyware)

Casus yazılımların ne şekilde bilgisayara bulaştığını kavrayan bir kullanıcı için, ikinci bir soru "Bu duruma bir daha düşmemek için, casus yazılımların sisteme bulaşmalarına engel olacak ne tür önlemler alınabilir?" olmalıdır. Takip eden bölümde bu soruya cevaplar aranmaya çalışılacaktır.

7. CASUS YAZILIMLARA KARŞI ALINABİLECEK ÖNLEMLER (PREVENTIVE MEASURES AGAINST SPYWARE)

Casus yazılımlara karşı alınabilecek önlemler, kullanıcıların kendilerinin alabileceği önlemler ve casussavar yazılımların sağladığı korunma olarak iki alanda incelenebilir. Bu çalışmada, kullanıcıların kendilerinin alabileceği önlemler ele alınmaktadır. Fakat casus yazılımlara karşı casussavar yazılımların kullanılmasının bir ön şart olduğunu vurgulamak gerekir.

Güvenlik konusunun işletim sistemi ve yazılım üreticileri tarafından birinci derecede ele alınması gerektiğinin ortaya çıkması ile bu konuda yapılan çalışmalar hızlandırılmış ve çeşitli güvenlik teknolojileri sunulmaya başlamıştır [13]. Casus yazılımlara karşı çok sayıda casussavar yazılım piyasaya sürülmekte ve kullanıcılar tarafından kullanılmaktadır [14]. Casussavar yazılımlar kötücül yapıları saptarken imza taraması ve ağ filtresi gibi klasik yaklaşımların yanı sıra erişim denetim listesini değerlendiren daha genel yöntemler de kullanılmaktadır [15].

Öncelikle, casus yazılımlara karşı tedbirli olmak için, sunulan önlemler bir alışkanlık haline getirilmelidir. Bu konuda sürekli olarak bilgilenmek, bir diğer önemli husustur. Aşağıda oldukça geniş bir yelpazede, alınabilecek önlemlerin en önemlileri listelenmektedir.

1) İşletim sistemi korunmasızlıklarını ve güvenlik açıklarını takip etmeye çalışınız.
2) İşletim sistemi ve programların hizmet paketlerini, yamalarını ve güncellemelerini düzenli bir şekilde sisteminize kurunuz. Windows işletim sisteminizin otomatik güncellemesi etkin bile olsa; kendiniz Windows Güncelleme sayfasını düzenli olarak ziyaret edip, önerilen güncellemeleri elle yükleyiniz.
3) Virüs tanımlama dosyalarınızın güncel olmasını sağlayınız. Önemli virüs uyarılarını dikkate alıp, sadece bu virüsler için çıkan virüs korunma programını indirip, tarama ve temizleme yapınız. Tüm sisteminizi düzenli aralıklarla tam taramadan (full scan) geçiriniz.
4) Mümkün oldukça lisanslı yazılım kullanınız. Lisanslı yazılımlar, güvenliği göz ardı etmeyen ve korunmasızlıkların en aza indirilmesine çalışıldığı yazılımlardır. Bu tür yazılımların, kullanıcılara hizmet veren müşteri destek kanalları da bulunmaktadır.
5) İnternet, casus yazılım bulaşma ortamlarının başında gelmektedir. Bu açıdan İnternet üzerinde gezinirken casus yazılımların uyguladığı ihlallere karşı dikkatli ve tedbirli olunuz [16].
6) MP3, warez ve crack gibi, aslında yasal olmayan siteleri ziyaret etmekten kaçınınız. Bu tip sitelerin

web yöneticilerinin, iş ahlakını düşündükleri pek söylenemez ve bu sitelere ait çoğu sayfanın HTML kodları arasında, gömülü bir casus yazılım bulunmaktadır.

7) BIOS önyükleme cihaz sıralamasını değiştiriniz. Diskinizde yer alan verilerinize istenmeyen kişilerin erişimini engellemenin önemli bir adımı da, BIOS'ta bulunan sistem başlatımının hangi cihazdan yapılacağını gösteren sıralamadır. Bu sıralamanın başında, disket sürücü, CD, DVD veya USB cihazlarının yerine, "sabit disk" seçilmelidir. Bu ayar BIOS'ta yapıldıktan sonra, BIOS'a bir şifre koyarak bu ayarın başkaları tarafından değiştirilmesinin önüne geçilebilir.
8) Her ne kadar Microsoft, tarayıcısı İnternet Gezgini'ni güvenli yapmaya çalışsa da; bu tarayıcı en çok kullanılan tarayıcı olma özelliği ile korsanların açıklarını yakalamaya çalıştıkları tarayıcıların başında gelmektedir. Bu ihtimali göz önüne alıp başka bir tarayıcı seçmeniz faydalı olabilir.
9) Zararlı web sitelerin bilgi toplamada kullandığı bir araç olan çerezlerle ilgili İnternet Gezgini izin ayarlarını ve güvenlik bölgelerini aşağıdaki şekilde ayarlayınız:
   - Birinci parti çerezleri sor ("Prompt for first-party cookies")
   - Üçüncü parti çerezleri engelle ("Block third-party cookies")
   - Oturum çerezlerine her zaman izin ver ("Always allow session cookies")
10) ActiveX betikleme ve Java betiklemeyi devre dışı bırakmak, bu tür ortamlara saldıran kötücül yazılımları durdurulabilir.
11) İnternet kafe'ler, üniversite yerleşkeleri ve oteller gibi umuma açık bilgisayarlarda, şifre, banka hesabı ve kredi kartı numarası gibi önemli verilerinizi kullandığınız işlemleri yapmamaya çalışınız. Bu tür bilgisayarlarda casus yazılım bulunabilir.
12) İnternet üzerinde çevrim içi alışveriş yaparken çok titiz ve şüpheci olunuz. Güvenilir ve güvenli protokollerle işlem yapan siteleri tercih ediniz.
13) Çevrim içi alışverişlerde kullandığınız kredi kartınızın limitini düşük tutunuz.
14) Düzenli aralıklarla kredi kartı dökümlerinizi madde madde inceleyiniz.
15) Şifre ve kimlik bilgileri gibi önemli bilgilerin bulunduğu not ve belgeleri olduğu gibi veya yırtarak çöpe ya da başka bir yere atmayınız. Bunun yerine kâğıt öğütücü makinelerini kullanınız.
16) Posta yolu ile gelen mektup ve belgelerinizi koruyunuz. Posta kutunuzu düzenli bir şekilde boşaltınız ve kilitli tutunuz.
17) Dizüstü bilgisayarınızın kasasına isminizi ve şirket adınızı yapıştırınız. Diz üstü bilgisayarınızı standart dizüstü çantaları yerine sıradan çanta veya bavul gibi gözüken modellerde taşıyınız. Dizüstü bilgisayarınızı görünecek şekilde arabanızın içinde bırakmayınız. Bilgisayarınızı mümkün olduğunca, yanınızdan ayırmayınız. Uçak ve otobüs seyahatlerinde dizüstü bilgisayarınızı kargo bölümüne vermeyip, yanınızda götürünüz. Kaldığınız otel odasında dizüstü bilgisayarınızı bırakmayınız.
18) Bilmediğiniz yazılımları indirmeyiniz ve kurmayınız. Programları güvenilir sitelerden indiriniz. Birçok casus yazılım diğer kurulum programlarının bire bir taklidini oluşturarak, istenilen program yerine kendisini kurabilmektedir.
19) Çıkıveren pencerelerdeki bir bağlantıya veya resme tıklamayınız. İşletim sisteminizin veya tarayıcınızın meşru mesajlarını okuyup ne dediği anlaşılmadan, "Evet", "Hayır", "Tamam" ve "İptal" gibi düğmelerine basmayınız.
20) Internet üzerinde gezinirken, aniden çıkan pencereleri kapatmak için pencere içindeki düğmeleri değil de; pencerenin sağ üst köşesindeki "X" şeklindeki kapat düğmesini veya Alt + F4 kapatma kısa yol tuşlarını kullanınız. Kötü niyetli kişiler bu tür pencerelerdeki masum görünen düğmeleri, kendi kötü amaçları için üzerlerinde yazandan farklı işlev görecek şekilde tasarlayabilirler.
21) Çocuklarınıza bilgisayar güvenliği ile ilgili bilgi veriniz. Onların daha güvenli bir şekilde İnternet'te gezinmelerini sağlayan önleyici programları kullanınız ve güvenli sistem ayarlarını yerine getiriniz.
22) Şüpheli gözüken e-posta eklentilerini asla açmayınız. Özellikle uzantıları .VBS, .SHS, .SCR, .EXE, .BAT, .COM, .PIF, .LNK, .SHB, .VB, .WSH, .WSF, .WSC, .SCT ve .HTA uzantılı dosyalar için çok dikkatli olunuz. Tanıdığınız birinden bile gelse, bu tür dosya eklentilerini en azından kaynağından doğrulatınız. Eklentilerin uzantılarının başka bir belge gibi gösterilebileceğini unutmayınız.
23) Outlook gibi bazı E-posta araçlarındaki "mesaj ön izleme" penceresini kapatınız. Bu şekilde gelen iletileriniz, listeden seçildiği zaman kendiliğinden açılmaz.
24) Gönderenin, konusunun ve büyüklüğünün şüpheli olduğu iletileri açmayınız.
25) E-posta aracınızın güvenlik ayarlarını sıkılaştırınız. Örneğin Outlook'ta "Tools > Options > Security > Secure content > Attachment security" kısmındaki eklenti güvenliğini (attachment security), Yüksek (High) yapınız. Bu şekilde eklentiler açılmak istendiğinde bir doğrulama iletisi gösterilerek, size eklenti hakkında düşünmenize ve eklentiyi açmaktan vazgeçmenize bir fırsat verilmiş olacaktır.
26) Mümkün oldukça e-postalarınızı "salt-metin" (in text only) olarak açınız.

27) Sosyal mühendislik veya toplum mühendisliği konusunda uyanık olunuz. Bu konuda güvenlik ile ilgili site, dergi ve bilgi kaynaklarını takip ediniz.
28) Şifre ve önemli bilgilerinizi kimseye vermeyiniz. Bunları bir kâğıda veya bilgisayarınızdaki bir dosyaya yazmayınız; yazdıysanız, bunları açıkta bırakmayınız.
29) İnternet'te göndereceğiniz eklentilerde, sizi ele verecek gizli bilgilerin olduğunu unutmayınız. Mesela göndermek istediğiniz bir Microsoft Word belgenizde isminiz, şirketiniz ve e-posta adresiniz otomatik olarak ekleniyor olabilir. Siz e-postanızı gönderdikten sonra bu belgenizin başka kimlere daha gönderilebileceğini bilemezsiniz. Bu tür gizli bilgileri elle siliniz veya mesela "Office 2003/XP Add-in: Remove Hidden Data" gibi programları kullanınız.
30) Windows işletim sistemde dosya yönetim programı olan Windows gezgini programında "gizli dosyaları göster seçeneğini" etkinleştirerek gizli olan klasör ve dosyaların görebilmesini sağlayınız. Ayrıca yine bu programın varsayılan ayarı olan "bilinen dosya türlerinin uzantılarını gösterme" (Hide file extension for known file types) seçeneğini kaldırınız. Aksi taktirde "zararsiz.txt.exe" isimli aslında çalıştırılabilir bir dosya, "zararsiz.txt" isminde bir metin dosyası olarak gözükeceğinden gözden kaçabilir.
31) Bu işleme rağmen uzantısı gösterilmeyen .SHS (Shell Scrap Object) dosyaları için, sistem kütüğünde HKEY_CLASSES_ROOT\ShellScrap anahtarında bulunan "NeverShowExt" değerini; .SHB (Document Shortcut) dosyaları için sistem kütüğünde HKEY_CLASSES_ROOT \DocShortcut anahtarında bulunan "NeverShowExt" değerini siliniz. Bu dosyalar, OLE (Object Linking and Embedding) teknolojisiyle kötücül yazılımların başka dosyalar içinde saklanması için kullanılabilmektedir.
32) Düzenli yedeklerinizi alınız.
33) Program kurulumlarından önce sistemi daha önceki haline getirmeye yarayan denetim noktaları oluşturunuz.
34) Sistem kütüğünüzü gereksiz girdilerden temizleyecek ve bütünlüğünü sağlayacak güvenilir programlar kullanınız. Bu şekilde kütük ile ilgili herhangi bir güvenlik açığına meydan vermeyeceğiniz gibi sistem başarımını da artırmış olacaksınız.
35) Makinenizin günlük kullanımında, yönetici hesabınızı kullanmayınız. Birçok casus yazılım, yönetici hesabı sistemde etkinken işlerini daha gizli ve daha ileri seviyede yapabilmektedir. Yönetici seviyesinde bir program çalıştırmak için "Run As" komutunu kullanabilirsiniz.
36) Çalışılmayan belli bir süre sonra şifre korumalı ekran koruyucusu çalıştıracak şekilde masaüstü değişikliklerini yapınız. Makinenizi bir süreliğine de olsa terk ederken kilitlemeyi unutmayınız. Windows XP ile birlikte klavyede (Microsoft) tuşu ile beraber L (Lock) tuşunu beraber kullanarak, bu işi hızlı bir şekilde yapabilirsiniz. Bu işlemi Windows 2000'de masaüstünde bir kısayol dosyasını "%windir%\System32\rundll32.exe user32.dll,LockWorkStation" şeklinde tanımlayıp. Buna, mesela CTRL + SHIFT + L şeklinde bir kısa yol tanımlayarak da yapabilirsiniz.
37) Kişisel bir güvenlik duvarı yazılımı kullanınız ve güncelleyiniz.
38) Kişisel bir casussavar yazılım kullanınız ve güncelleyiniz.

Bir programı satın alırken, kurmadan önce veya kullanırken programın casus yazılım olup olmadığını aşağıdaki soruları cevaplayarak bulmak mümkün olabilmektedir [17]. Bu sorular,

1) Program kullanıcıya bilgi vermeden sistem faaliyetlerinin kaydını tutuyor mu?
2) Uygulama iyi anlaşılmayan veya aşırı hukuki ifadelerin olduğu bir "Uç Kullanıcı Lisans Anlaşması" mı içeriyor?
3) Lisans anlaşması son kullanıcı tarafından anlaşılmayan bir mesleki dil (jargon) mi kullanıyor? Örneğin çıkıveren pencereler için "interstitials" veya "daughter consoles" gibi terimler kullanılıyor olabilir.
4) Uygulama dağıtım için kaçak indirme yöntemi mi kullanıyor?
5) Uygulama yayılma için bilinen veya bilinmeyen güvenlik boşluklarından yararlanmaya çalışıyor mu?
6) Popüler teknik forumlarda uygulama hakkında yoğun şikâyetler var mı?
7) Uygulama izinsiz başlangıç sayfası veya arama ayarlarını değiştiriyor mu?
8) Uygulama ismini, bilinen standart bir Windows işletim sistemi dosyası ismine değiştirme veya program kaldırılmasının önlenmesi gibi gizlenme taktikleri kullanıyor mu?
9) Kaba kuvvetle program kaldırıldığında, LSP (Layered Service Provider, Katmanlı Hizmet Sağlayıcı) yığınını kırmak gibi bilgisayarın işlevine ağır yükler bindiriyor mu?
10) Kullanıcı tarafından program kaldırıldığında kendini tekrar kurmak için "damlatıcı programı" gibi programlar kullanıyor mu?
11) Program üreticileri programın kaldırılması için kullanıcıdan zorla ücret talep ediyor mu?

olarak sıralanabilir. Aşağıda belirtilen önlemler de daha çok sistem veya ağ yöneticilerin alabileceği önlemlerdir:

1) Yeni tehditlerden ve saldırı tekniklerinden haberdar olmak için gerekli girişimlerde

bulununuz. Örneğin teknik forumlara üye olunuz ve güvenlik ile ilgili bültenlere abone olunuz.

2) En son güncellemeleri takip ediniz ve sisteminize vakit geçirmeden uygulayınız.
3) E-posta sunucunuzda ".exe, .pif, .scr ve .vbs" gibi kötücül yazılım dağıtımına müsait dosyalara engel koyunuz.
4) Sistemdeki kullanıcılarınızı düzenli aralıklarla eğitiniz. Yeni tehditlere karşı uyarınız.
5) Kullanıcılara yetecek kadar haklar veriniz.
6) Kullanıcıların önemli verilere erişimlerini kısıtlayınız.
7) Bir güvenlik politikası oluşturunuz ve güncelleyiniz. Bu politikaya uyulup uyulmadığını kontrol ediniz.
8) Uzaktan erişim ile ilgili riskleri analiz edip önlemler alınız.
9) Saldırı ve hasarlara karşı bir yıkım onarımı planı hazırlayınız.

Çocuklarınız için ise farklı kurallar belirlemenizde fayda vardır. Microsoft'un bu konudaki bazı uyarılar özetlenmiştir [18].

- Çocukların internet kullanım kurallarına uygun olarak web ortamında gezinmesini sağlayınız.
- Internet'e bağlı olan bilgisayarları çocuklarınızın yatak odalarının dışında tutunuz.
- Çocuklarınızla etkinlikleri hakkında konuşunuz ve yabancılarla iletişim kurmalarını engelleyiniz.
- Ebeveyn gözetimine yardımcı olmak amacıyla internet filtreleme araçlarını kullanınız.
- Çocuklarınızın hangi sohbet odalarını ya da ileti panolarını ziyaret ettiğini ve çevrimiçi ortamda kimlerle iletişim kurduğunu takip eden programlar kullananınız.
- Çevrimiçi ortamda edindikleri arkadaşlarla asla gerçek yaşamda buluşmamaları için öğütlerde bulununuz.
- Çocuklarınıza e-posta, sohbet odası ya da anlık ileti kullanırken, kayıt formu ve kişisel bilgilerini vermemeleri öğretiniz.
- Çocuklarınızın izniniz olmadan program, müzik ya da dosya indirmesine müsaade etmeyiniz.
- Çocuklarınızı, çevrimiçi ortamda kendilerini rahatsız ya da tehdit altında hissettiren bir şey ya da bir kişi olduğunda size iletmelerini salık veriniz.
- Çevrimiçi saldırganlar ve sanal kabadayılarla nasıl baş edebileceğinize ilişkin güncel yayınları okuyunuz.
- Onları istenmeyen postalardan koruyunuz. Çocuklarınıza çevrimiçi ortamda e-posta adreslerini vermemelerini, istenmeyen postalara yanıt vermemelerini ve e-posta filtresi kullanmalarını anlatınız.
- Çocuklarınıza ziyaret etmesi gerekli siteleri öneriniz.
- Kötü içerikli siteleri ziyaret etmemesini ya da kişisel bilgilerini ya da fotoğraflarını kimseye iletmemelerini ve zamanlarını boşa harcamamaları yönünde çocuklarınızı bilgilendiriniz.
- Çocuklarınızın bilgisayarında lisanslı yazılımlar kurunuz.
- Mutlaka anti-virüs, anti-casus ve anti-spam yazılımlarının kurulu olmasına ve bu yazılımların sık sık güncellenmelerini sağlayınız.

8. SONUÇ VE DEĞERLENDİRME (CONCLUSION)

Bu çalışmada, bilgi ve bilgisayar güvenliğine yönelik en büyük tehditlerden biri olan casus yazılımlar, somut örneklerle ele alınmıştır. Casus yazılımlar ve diğer kötücül yazılımlar; sayı, çeşitlilik ve kullandıkları yöntem bakımından sürekli bir artış halindedir. Bu yazılımların ve kullandıkları yöntemlerin yakın ve sıkı bir şekilde takip edilmesi gereklidir. Çalışmada casus yazılımların bilgisayar sistemlerine sızabilmek ve zarar verebilmek için ne gibi yöntemler kullandıkları incelenmiş ve karşılaşılabilecek çok ilginç durumlar gözler önüne serilmiştir. İşin boyutlarını algılamak açısından bu çalışmada sunulan örneklerin oldukça faydalı olacağı değerlendirilmektedir.

Çalışmada elde edilen en önemli bulgulardan biri, bu tür yazılımları yaymak isteyen kişilerin oldukça kötü niyetli oldukları ve kullanıcıları tuzağa düşürmek için akla gelmedik hilelere başvurduklarıdır. Casus yazılımlara karşı gerek işletim sistemi bazında gerekse bu tür yazılımlardan korunma amacıyla geliştirilen koruma yazılımların kullanılması ve bu kullanımın yaygınlaştırılması önemli bir konudur. Ayrıca kurumsal seviyede sistem yöneticilerine ve güvenlik uzmanlarına büyük işler düşmektedir.
Ancak, sadece bu tür önlemlerle yetinmek karşılaşılabilecek her türlü sorunu çözmek için yeterli değildir. Bu konuda başta çocuklar ve sıradan ev kullanıcıları olmak üzere şirket ve kurum çalışanlarının bilinçlendirilmesi ve bu tür hilelere karşı uyanık olmaları şarttır. Çocuklarımızın güvenliğini tehlikeye atmamamız gerektiğini, kullandıkları yazılım ve donanımları onlara uygun olarak hazırlamak ve güvenli olarak kullanımlarını sağlamamız gerektiğini de hatırımızdan çıkarmamalıyız.

Ayrıca bu çalışmada özgün bir şekilde ve geniş bir kapsamda önerilen önlemlerin kullanıcılar tarafından sürekli ve titiz bir biçimde tatbik edilmesi gereklidir. Bu konuya verilecek önem ileride karşılaşılabilecek sorunların önüne geçmeye, kayıpların azaltılmasına, kişisel bilgi ve bilgisayar güvenliğinin daha yüksek seviyede sağlanmasına yardımcı olacaktır.

KAYNAKLAR (REFERENCES)

1. Canbek, G., Sağıroğlu, Ş., **Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri: Bir İnceleme**, Erciyes Üniversitesi, Fen Bilimleri Dergisi, Cilt : 22, Sayı : 1–2, Basımda, 2007.
2. Canbek, G., Sağıroğlu, Ş., **Kötücül ve Casus Yazılımlar : Kapsamlı Bir Araştırma**, Gazi Müh. Mim. Fak. Dergisi, Cilt 22, No: 1, sayfa 121–136, Mart 2007, Ankara, Türkiye.
3. Canbek, G., Sağıroğlu, Ş., **Bilgisayar Güvenliği ve Casus Yazılımlar Kapsamında Kişisel Gizlilik ve Yasal Düzenlemeler**, Savunma Bilimleri Dergisi, KHO Savunma Bilimleri Enstitüsü, İncelemede, 2007.
4. **State of Spyware Report – 2005**, Webroot, 2006.
5. Canbek, G., **Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme**, Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Eylül 2005, Ankara.
6. **Monitoring Software on Your PC: Spyware, Adware, and Other Software, Staff Report**, Federal Trade Commission, Mart 2005.
7. Canbek, G., Sağıroğlu, Ş., **Çocukların ve Gençlerin Bilgisayar ve İnternet Güvenliği**, Politeknik Dergisi, Teknik Eğitim Fakültesi, Gazi Üniversitesi, Cilt 10, No: 1, sayfa 33–39, Ocak 2007, Ankara.
8. İnternet: Magid L., **It Pays To Read License Agreements**, PC Pitstop Newsletter, February 2005, http://www.pcpitstop.com/spycheck/eula.asp (Eylül 2007).
9. İnternet: Edelman B., **Gator's EULA Gone Bad**, 29 Kasım 2004, http://www.benedelman.org/news/112904-1.html (Eylül 2007).
10. İnternet: Bailey B., **Optimal Line Length**, UI Design Newsletter, Human Factors International Inc., Kasım 2002. http://www.humanfactors.com/downloads/nov02.asp#tpe (Eylül 2007).
11. İnternet: Edelman B., **Comparison of Unwanted Software Installed by P2P Programs**, Mart 2005, http://www.benedelman.org/spyware/p2p/ (08.05.2005).
12. İnternet: McClellan, J., **Spies at liberty in your PC**, The Guardian, http://technology.guardian.co.uk/online/story/0,3605,744203,00.html, 27 Haziran 2002, (Eylül 2007).
13. Lee Y., Kozar K. A., **Investigating Factors Affecting Adoption of Anti Spyware Systems**, Vol. 48, No. 8, pp 72–77, Communications of The ACM, Ağustos 2005.
14. Poston R, Stafford T.F., and Hennington A., **Spyware: A View the (Online)**, Vol. 48, No. 8, pp 96–99, Communications of The ACM, Ağustos 2005.
15. Chow S. S. M., Hui L. C. K., Yiu S. M., Chow K. P., Lui R. W. C., **A generic anti-spyware solution by access control list at kernel level**, The Journal of Systems and Software, 75 (2005) 227–234.
16. Shukla, S., Nah F.F.H, **Web Browsing and Spyware Intrusion**, Communications of The ACM, Vol. 48, No. 8, pp 85–90, Ağustos 2005.
17. İnternet: **Tough Questions and Bad Behavior**, FaceTime Communications, Inc., 2005. http://www.spywareguide.com/articles/tough_questions_and_bad_behavi_37.html (Eylül 2007).
18. **Ebeveynler için çevrimiçi güvenlik kılavuzu: Yaşlar ve dönemler**, http://www.microsoft.com/turkiye/athome/security/children/parentsguide.mspx, 14 Aralık 2004, (Eylül 2007)