ReadJournal
GAZETE : İTOVİZYON
SAYFA NO : 68
TARİH : 17 Ekim 2012 Çarşamba
BÖLÜM : KONUK YAZAR - GUEST WRITER
itovizyon

KONUK YAZAR-GUEST WRITER

Prof. Dr. Çetin Kaya Koç

DÜŞÜN VE SONRA "TIK"LA

THINK BEFORE YOU 'CLICK'

Casus yazılımın sahipleri, sizden habersiz veya sizden izin almadan Internet üzerindeki hareketlerinizi izlediği gibi, klavyede bastığınız her tuşu, parola ve PIN numaralarınızı öğreniyor ve bilgisayardaki değerli bilgilerinizi çalıyor. O nedenle "tık"lamadan önce düşünün.

Owners of the spyware program can obtain your passwords and PIN numbers, follow each stroke of your keyboard, and your actions on the internet, all without your permission or knowledge. So think before , you 'click'.

Spyware – casus yazılım; genellikle kullanıcının haberi bile olmadan veya haberi olsa bile programın neler yaptığı kullanıcıya tam açıklanmadan bilgisayarına yüklenen programlara verilen isim. Casus yazılımların bir kısmı kullanıcı hakkında pazarlama bilgileri toplamak amacında; okuduğunuz yayınları veya alış veriş ettiğiniz ticari amaçlı web sitelerini, abone olduğunuz sosyal medya sitelerini ve eğilimlerinizi kaydediyor; bunları casus yazılım sahiplerine iletiyor. Ancak önemli bir kısmı çok daha zararlı; casus yazılımın sahipleri, sizden habersiz veya sizden izin almadan Internet üzerindeki hareketlerinizi izlediği gibi, klavyede bastığınız her tuşu, parola ve PIN numaralarınızı öğreniyor ve bilgisayardaki değerli bilgilerinizi çalıyor.

Ne yazık ki casus yazılımları önlemenin tek ve etkili bir yolu yok. Casus yazılımı bilgisayarınızdan çıkarıp atma işine odaklanmış firma veya kişilerin hizmetlerinden faydalanmak mümkün. Bir çok kullanıcı, casus yazılımı çıkarıp atmak yerine bilgisayarlarını

Spyware is the name given to programs installed on the computer of a user without their knowledge, or even if it is with their knowledge, without a full explanation of what it does. Some spyware has the goal of collecting marketing information about the user, and records the publications you read, the websites you shop from, the social media sites you subscribe to, and your computing tendencies, delivering this information to the developers of the spyware program. However, a substantial portion of spyware is designed to be much more harmful; owners of the spyware program can obtain your passwords and PIN numbers, follow each stroke of your keyboard, and your actions on the internet, all without your permission or knowledge.

çöpe atmayı bile tercih etmekte. Uzun vadeli çözümler zahmetli ve karmaşık: hukuki düzenlemeler yapmak ve kullanıcıları sürekli olarak eğitmek gerekiyor.

NASIL BULAŞIYOR?

Casus yazılımlar bir kaç noktadan bilgisayarınıza yerleşebilir, örneğin, e-postadaki bir linke tıklayınca veya tarayıcı ile uğradığınız bir web sitesinden direkt olarak veya site içinde bir linke tıklayınca.

Özellikle pazarlama amaçlı casus yazılım dağıtıcıları, siz söz konusu siteye gidince size sormadan casus yazılımı yükleyebilir. Aslında tarayıcının prensip olarak buna izin vermemesi gerekiyor; ancak bazı tarayıcı programlarındaki zayıflıkları istismar eden casus program yazıcıları, kullanıcıdan habersiz tarayıcının casus yazılımı yüklemesini sağlıyor. Bu programların en masum olanları, tarayıcının başlangıç sayfasını değiştirip, sürekli ortaya çıkan minik pencereler yaratmakta.Ancak daha ciddi zararlar, örneğin, kullanıcının Internet aktivitesinin kaydı ve formlara yazdığınız bilgilerin (isim, adres, kredi kartı bilgisi gibi) çalınması söz konusu.

BEDAVA TUZAĞI

Tam bu noktada, casus yazılımın sadece masaüstü bilgisayarlar değil aynı zamanda akıllı telefonları da içerdiğini belirtmekte yarar var. Mobil cihazlara saldırı yoğunluğu gittikçe artmaya başladı. Bedava uygulamalar saldırının en kolay yolu. Hırsızı evinize siz davet ediyorsunuz. Diyelim ki telefonunuzda bir mobil bankacılık uygulaması var; telefon "jailbreak" yapılmış ise, herhangi bir uygulama mobil bankacılık uygulamasına ait alanı okuyabilir, müşteri numarası, şifre ve parolanın hepsini kolaylıkla elde edebilir.

ABD Standartlar Enstitüsü (NIST: National Institute of Standards and Technology) yakın bir zamanda yaptığı bir araştırmayı yayınladı. 280 bin bedava mobil uygulamayı inceleyen NIST bunlardan 2 bin tanesinde casus yazılım tespit etti. Türkiye'de akıllı telefonlara bedava uygulama koyma merakı çok yüksek ve hatta sadece bu nedenle telefonunu 'jailbreak' yapan bir çok kişi var. O yüzden konu bizi de ilgilendiriyor. NIST araştırmasına göre mobil uygulamaların yüzde 1i çok bariz bir şekilde casus yazılım. Bunların sayısı her gün hızla artıyor. Bir takım faydalı fonksiyonları bedava sunduğu için tercih edilen bu uygulamalar yüzünden kullanıcılar mağdur oluyorlar; kişisel verileri çalınıyor.

ABD'nin Federal Ticaret Kurumu (FTC: Federal Trade Commission), casus yazılım konusunda ciddi çalışmalar yapıyor. FTC, bir çok casus yazılım ve bilgi toplama

Unfortunately, there is no single effective way to prevent spyware. It is possible to make use of the services of individuals or companies who find and remove spyware from your computer. Many users prefer to throw away their computers instead of removing spyware. Long-term solutions are difficult and complicated to implement; therefore, it is necessary to make legal arrangements and educate users.

HOW CAN YOU BE INFECTED?

Spyware can install itself on your computer from a few sources. For instance, when you click on a link in an e-mail, or directly from a website you've visited in your browser, or if you click on a link inside a site. Those who distribute spyware for marketing purposes are able to install spyware without your permission when you enter a site. Actually, in principle, the browser should not give permission for this; however, spyware programmers can exploit the weaknesses of some browsers to ensure the browser installs the spyware without the knowledge of the user. The most innocent of these programs can change the homepage of the browser, and create never-ending pop-up windows. However, it is also possible to cause more significant damage, such as capturing the Internet activity log of the user and the information that is typed into forms, such as name, address, and credit card information.

THE "FREE" TRAP

At this point, it would be beneficial to state that spyware does not just affect desktop computers; it also affects smart phones. The intensity of attacks on mobile devices has been increasing more and more lately. Free applications are the easiest method of attack. You invite the thief into your home yourself. For example, if there is a mobile banking application on your phone and your phone has been "jailbroken", any application on the phone can read the memory space belonging to the mobile banking application, and easily obtain the customer number, password, and security code.

The U.S. National Institute of Standards and Technology recently published a report on its spyware research. NIST studied 280,000 free mobile phone applications and determined that 2,000 of them had spyware. The interest in installing free applications on smart phones is high in Turkey, and in fact, for this reason alone, there are many people who "jailbreak" phones. It is for this reason that this topic is significant for us as well. According to the NIST research, 1% of all mobile applications

firmasını mahkemeye verdi ve onların bazı çalışmalarına engel oldu. Kullanıcıya haber vermeden program yükleme veya kullanıcıya programın yaptığı diğer fonksiyonlardan bahsedilmemesi gibi konularda mahkemelerde davalar açarak ve bunları başarı ile sonuçlandırarak tüketicileri casus yazılımdan koruma konusunda çok faydalı çalışmalar yaptı ve yapmaya devam ediyor.

YASAL GÜVENCE SINIRLI

Casus yazılım ve pazarlama bilgisi toplama firmalarının çoğu ABD kökenli olduğu için hukuki düzeyde çalışmalar yapmak ve sınırı aşan firmaları mahkemeler yoluyla engellemek en azından teorik olarak mümkün. Ancak, sadece pazarlama bilgisi toparlayan casus yazılımların durumu, özellikle, bu bilgilerin kullanıcı kimliğinden bağımsız yapılması durumunda, hukuki olarak gri noktada; böyle durumlarda mahkemeler pek etkili olamıyor. Diğer yandan, kullanıcıya ait gizli kalması gereken bilgilerin casus yazılımlarla çalınması kesin olarak hukuka aykırı. Bu konular ABD'de ve Avrupa ülkelerinde mahremiyet kapsamındaki kanunlarla düzenlenmiş. Fakat bu işlerle meşgul (kamuoyunun kötü niyetli hacker dediği) kişi veya grupların çoğunun ABD veya Avrupa dışında olması veya kimlik ve çalışma yerlerini saklamaları, bunlarla baş etmeyi zorlaştırıyor. Görüldüğü gibi casus yazılımlar konusunda hukuksal ve kanuni düzenlemelerin başarı şansı sınırlı.

Ayrıca konu teknik olarak sürekli akış ve gelişme içinde; casus yazılım üretenler, işletim sistemleri, ağ ve yazım teknolojilerini çok yakından ve hatta akademisyenlerden de çok daha ilerde takip edip faydalanıyorlar. Onlarla mücadele etmek, her yeni casus

yazılım metodunu öğrenmek ve buna karşı gerekli hukuksal girişimlerde bulunmak her zaman mümkün ve yeterli değil.

Casus yazılım sadece tüketicilere zarar veren bir olgu değil; kurumlar ve şirketler de zarar görebiliyorlar. Doğrudan tasarım şirketlerini saldırıya odaklanmış casus yazılımlar var. Burada özellikle "kırılmış tasarım programı" edinmeye dönük eğilimlerin ortaya çıkardığı problemlerden bahsetmekte yarar görüyorum. Bazı bilgisayarla tasarım programlarının fiyatını yüksek bulan tasarımcılar, yazılımı üreten firmasından satın almak yerine, daha ucuz bir fiyata veya bazen bedavaya onun "kırılmış" halini tercih etmekte. Ne yazık ki böyle programların içindeki casus yazılım bölümleri tasarımcının büyük bir zaman ve emek yatırımıyla geliştirdiği tasarımları çalmak amacıyla yazılmış. ABD ve Avrupa'da bunun bir çok örnekleri ortaya çıktı ve tasarımcılar mağdur durumlara düştüler.

TÜKETİCİYİ BUNALTIYOR

Kurum ve şirketlerin bir diğer zararı, casus yazılım programlarının ortaya çıkardığı güvenilmez ve şüpheci ortamın tüketicileri yorması ve onların ilgisini azaltması. Dolayısıyla

are clearly spyware programs, and the number is increasing rapidly everyday. Users choose these applications because they offer some useful functions for free, but they end up becoming victims, with their personal information being stolen.

The U.S. Federal Trade Commission has done some important work on the issue of spyware. The FTC has taken many spyware and information-gathering companies to court, preventing some of them from doing business. They have filed court cases against spyware producers on the basis of installing a program without informing the user or not mentioning hidden functions a program performs without the user's knowledge. The successful completion of these cases has led to some useful measures being taken to protect the consumer from spyware.

LEGAL PROTECTION IS LIMITED

Because most of the companies who develop spyware and gather marketing information are of U.S. origin, it is possible in theory to take legal action against the companies who break the law. However, the situation of spyware that only collects information for marketing purposes is in a legal gray zone, especially if the collection of this information is done without tracking the users' identity, and courts cannot be really effective in situations like this. On the other hand, it is absolutely illegal for user information that should remain secret to be stolen via spyware. These crimes are regulated through privacy protection laws in the U.S. and European countries. However, because most individuals or groups that commit such acts, whom the public refers to as ill-intended hackers, are located outside the U.S. and Europe, or because they keep their identities and locations hidden, it becomes difficult to deal with them. It is easy to see that the possibility of success for legal and statutory regulations in such cases is very slim.

Moreover, the spyware constantly develops and changes technically. Those who develop spyware follow changes to operating systems, networks, and software technologies even more closely than academics, and in fact, they benefit from such changes. To fight them, to learn each new spyware method, and to take legal action is not always possible and not always sufficient.

Spyware does not only harm consumers; it also affects institutions and companies. For example, there are spyware programs that directly focus on attacking design companies. Here especially, I find it beneficial to mention the problems arising from the tendency to obtain cracked design programs. Designers who find the prices of some computer design software programs expensive prefer to find a "cracked" version cheaper or sometimes for free, instead of purchasing the program from the developer. Unfortunately, the spyware

bunun direkt olarak iş hacminin daralmasına neden olması. ABD'de bir çok tüketici casus yazılımdan uzak durmak için Internet alışveriş etkinliğinden de uzak durmayı tercih etmekte. Bu konuda yapılan bir ankete göre, tüketicilerin yüzde 90'ı davranışlarını bir miktar değiştirmeyi seçmiş; diğer yandan yüzde 48'i bazı web sitelerine bu yüzden artık kesinlikle gitmediklerini ifade ediyor.

Casus yazılımlar nedeniyle, tüketici güveninin azalması özellikle küçük firmalara ve yeni başlayan firma ve şirketlere çok zarar vermekte. Üstelik, casus yazılım metodunu seçen pazarlama ve reklam firmaları da bundan payını alıyor; kullandıkları silah (deyim yerindeyse) kendilerine zarar verdiğini gözlemliyoruz.

KAYNAK YURTDIŞI OLABİLİR

Görüldüğü gibi casus yazılım konusu çok geniş ve iş hayatına olan zararları çok bariz. "Casus yazılım gelişmeleri genellikle bir ABD veya Avrupa konusudur; bizi pek ilgilendirmez" dememiz hiç doğru değil. Pazarlama bilgisi toplama veya hırsızlık amacı ile casus yazılım geliştirenler Türkiye dışında olabilir; ancak ülkemiz içinde insanlarımız ve şirketlerimiz mağdur oluyorlar.

Casus yazılımla mücadelenin çok yönlü olması gerekiyor. Bir yandan kötü niyetli kişi ve gruplara hukuki bir şekilde engel olmaya çalışırken, diğer yandan bunlardan zarar gören kişi ve kurumları eğitmek gerekiyor. Bu konuda bilgisayar güvenliği uzmanları, online alışveriş firmaları, tüketici koruma dernek ve kurumları ve emniyet teşkilatına bir çok görevler düşüyor.

Bu yazının başlığını ABD federal ticaret kurumunun "Stop ThinkClick[1]" isimli kampanyasından esinlenerek seçtim. Burada amaç tüketicileri casus yazılımlar hakkında bilgilendirmek ve onları kötü amaçlı web sitelerinden uzak tutmak, e-posta ile gelen her şeye inanmamalarını sağlamak. Gerçekten de "tık"lamadan önce düşünmemiz gerekiyor.

1 http://onguardonline.gov

inside such "cracked" programs were written with the purpose of stealing the designs of the designer, which could have been required a lot of time and effort. Many examples of designers being victimized in this way have been seen in the U.S. and Europe.

THE CONSUMER IS OVERWHELMED

One other harm spyware inflicts on institutions and companies is that the unreliable and suspicious environment created by spyware programs overwhelms consumers and causes their interest to diminish. In the U.S., many consumers refrain from shopping online because they want to avoid spyware. According to a survey conducted on this topic, 90% of consumers chose to change their habits, while 48% stated that they do not log onto certain websites because of this reason. The loss of consumer trust due to spyware programs damages smaller companies and newly emerging companies more so than others. Moreover, marketing and advertising companies which prefer to use spyware methods also lose trust, thus, they end up shooting themselves in the foot.

THE SOURCE MIGHT COME FROM ABROAD

As can be seen, the topic of spyware programming is a large one, and its harmful effect on business life is extremely clear. To state that the developments in spyware programming are generally limited to the U.S. or Europe and that they do not concern us would not be right. Those developing spyware for the purpose of collecting marketing information or theft might be from outside the country, but the people living in our country and our own companies are the ones being victimized.

The struggle against spyware needs to be multifaceted. On one hand, it is important to use legal methods to prevent individuals and groups from distributing spyware, and on the other, it is also necessary to educate individuals and institutions that are being harmed by spyware. In this matter, responsibility falls on the shoulders of computer security experts, online shopping companies, consumer rights agencies, and the security forces.

While deciding on the headline for this article, I was inspired by the U.S. Federal Trade Commission's campaign titled "Stop, Think, Click[1]." The goal here is to inform consumers about spyware programs, keep them away from harmful web sites, and ensure that they do not believe everything they receive via e-mail.

And we really do need to think before we click.

1 http://onguardonline.gov