Kötücül Yazılımlar - 2 (Casus Yazılımlar, Keyloggerlar, Botnetler)

Casus yazılım (Spyware), tanıtım, kişisel bilgi toplama veya onayınızı almadan bilgisayarınızın yapılandırmasını değiştirme gibi belirli davranışları gerçekleştiren yazılımlar için kullanılan genel bir terimdir.

Casus yazılım (Spyware), tanıtım, kişisel bilgi toplama veya onayınızı almadan bilgisayarınızın yapılandırmasını değiştirme gibi belirli davranışları gerçekleştiren yazılımlar için kullanılan genel bir terimdir.

Casus yazılımlar genellikle, reklam pencereleri görüntüleyen yazılımla (reklam yazılımı) ya da kişisel veya önemli bilgileri izleyen yazılımla ilişkilendirilir. Bu, reklam sağlayan veya çevrimiçi etkinliklerinizi izleyen her yazılımın kötü olduğu anlamına gelmez. Örneğin, hedeflenen reklamları almayı kabul etmeniz "karşılığında" bir müzik hizmetine ücretsiz kaydolabilirsiniz. Koşullarını anladıktan ve kabul ettikten sonra, bunun adil bir anlaşma olduğuna karar verebilirsiniz. Ayrıca şirketin sizin için görüntüleyeceği reklamlara karar vermesi için çevrimiçi etkinliklerinizi izlemesine izin vermeyi de kabul edebilirsiniz. Diğer istenmeyen yazılım çeşitleri bilgisayarınızda rahatsız edici değişiklikler yapabilir ve bilgisayarınızın yavaşlamasına veya kilitlenmesine neden olabilir. Bu programlar, web tarayıcınızın giriş sayfasını veya arama sayfasını değiştirebilir ya da tarayıcınıza istemediğiniz veya gerek duymadığınız ek bileşenler ekleyebilir.

Casus Yazılım Bulaşma Belirtileri

1. Sık sık pop-up pencere açılması.
2. Kontrolsüz çalışan web tarayıcısı.
3. Ana sayfa olarak ayarladığınız adresin değişmesi.
4. Yeni ve sizin yüklemediğiniz web tarayıcı çubukları.
5. Programların çok ağır veya yavaş çalışması.

Casus yazılımlardan korunmak için anti-virüs yazılımları, internet güvenlik yazılımları ve casus yazılımları bulup yok eden çeşitli programlar kullanılabilir.

Keyloggerlar, klavyeden basılan her tuşun loglarını tutan casus yazılımlardır. Bu yazılımlar siz internette gezinirken gireceğiniz parolaları ve kişisel bilgilerinizi bir metin dosyasına kaydedip başka bir kullanıcıya ulaştırır.

Keyloggerlar nasıl tespit edilir ve nasıl kurtulunur?

Piyasada birçok keylogger bulunmaktadır ve her keylogger değişik bir mantıkla log tutmaktadır. Bu yüzden hepsinden aynı yöntemle kurtulmak mümkün değildir. Basit bir keyloggerdan kurtulmak için Baslat>Çalıştır>msconfig yazıp açılan pencereden "Başlangıç" sekmesine gelerek listede açılışta çalışmaya başlayan programları görerek keylogger'ları tespit edip çalışmasını durdurabilirsiniz. Bu durumda bütün işlemleri devre dışı bırak bilgisayarınızı yeniden başlatınız. Ayrıca; Ctrl + alt + delete tuşlarına basıp "işlemler" menüsünde services.exe karşısında SYSTEM yerine admin vs. yazıyorsa sisteminizde keylogger olabilir. c:/windows/system32 klasörünüzde SystemDll32.exe ve SystemDll32.log dosyalarını görüyorsanız bilgisayarınızda yine keylogger olabilir. Bu durumda Bilgisayarım/C/windows/system klasörünüzdeki services.exe yi silin. Yine de casus yazılımlardan en etkin kurtulma yöntemi bilgisayarınıza format atmaktan geçmektedir

Casus Yazılımlardan Korunma Yöntemleri

- İşletim sistemi ve web tarayıcı yazılımlarınızı güncelleyin.
- Anti-virüs yazılımları, internet güvenlik yazılımları ve casus yazılımları programları kullanın. İşletim sisteminizin güvenlik duvarını aktif hale getirin.

- Ücretsiz yazılımları bildiğiniz ve güvendiğiniz yerlerden edinin.
- Ne işe yaradığını bilmediğiniz yazılımları bilgisayarınıza yüklemeyin.
- Web tarayıcı gizlilik ve güvenlik ayarlarınızı kontrol edin.
- Ne işe yaradığı belli olmayan pop-up pencerelere tıklamayın.
- İstenmeyen ziyaretçilerin bilgisayarınıza erişimi engellemek için güvenlik duvarı (firewall)yükleyin.
- Casus yazılım bulaştığından şüpheleniyorsanız internet üzerinden bankacılık gibi kritik işlemlerinizi kullanmayın.

Bilgisayar kullanımının yaygınlaşması ile bilgisayarlara yapılan saldırı ve tekniklerde gün geçtikçe artmaktadır. Ağ saldırılarının en tehlikelilerinden olan BotNet saldırısı ile bilgisayar korsanları kişisel bilgisayarları ele geçirebilmektedir. Botnet son dönemlerde bir hayli yaygınlaşmış olmakla beraber, web üzerinden e-ticaret yapan firmalar, Kamu Kurumları ve diğer hizmet sağlayıcı kurum ve kuruluşlar Botnetlere maruz kalabilmektedir.

Botnet saldırıları, temelde birçok bilgisayarın tek bir noktadan kötü amaçlar doğrultusunda yönetilmesi demektir. Bir tür virüs ile bilgisayarınıza bulaştırılan erişim programları ile kötü niyetli bilgisayar korsanlarının binlerce zombiden oluşan ordusuna kolay bir şekilde katılabilirsiniz. Bir Botnet sahibi saldırgan, ağındaki tüm bilgisayarları dünyanın herhangi bir yerinden kolay bir şekilde yönetebiliyor. Botnet ağındaki masum kullanıcılarda, saldırganların siber suçlarına haberleri bile olmadan büyük destek oluşturuyor.

Botnet'lerden Korunma Yöntemleri

- Bilgisayarınızda yüklü olan anti-virüs programının güncel olduğundan ve/veya programın kendini otomatik güncellediğinden emin olun.
- İnternet üzerinden gelen trafiği sürekli denetim altında tutan firewall (güvenlik duvarı) yazılımları kullanın.
- İnternetten bir program indirirken çok dikkatli olunuz. İndirdiğiniz programının güvenilirliğinden, indirdiğiniz web sayfanın bilinilirliği ve güvenilirliğinden ve her şeyden önce indirdiğiniz programı virüs taramasından geçirdiğinizden emin olunuz.
- İşletim sisteminizin güncel olduğuna ve en son güncellemelerin yüklü olduğuna emin olunuz. Örneğin Windows 7 işletim sistemi kullanıyorsanız Başlat –Denetim Masası – Sistem ve Güvenlik – Windows Update adımlarınızdan işletim sisteminizin güncel olup olmadığının öğrenebilirsiniz.
- E-Posta ile gelen dosyalara devamlı şüphe ile yaklaşın. Dosya uzantısı .pif, .scr, .bat, .exe, .zip, .rar ise dikkatli olun. Eğer dosyanın uzantısından emin olamıyorsanız, Windows İşletim Sistemleri için Klasör Seçenekleri altında yer alan Görünüm bölümündeki "Bilinen dosya türleri için uzantıları gizle" seçeneğini kaldırınız.

ETİKETLER

#KötücülYazılımlar #CasusYazılımlar