Siber Güvenlik Nedir ?

Bilişim sistemlerinde insanlarla veya kurumlar arası kurduğumuz iletişimin, yaşamın, entegrasyonun, maddi veya manevi varlıklarımızın hatta elektronik ortamdaki verilerimizin güvenliğinin, bütünlüğünün ve gizliliğinin korunmasıdır.

Günümüz teknoloji çağında, hayatımızın büyük bir kısmını elektronik ortamlarda yansıtmaya ve yaşamaya başlamış durumdayız. Yalnızca biz bireyler değil! Devletler, kamu kurumları, sosyal platformlar, kobiler, irili ufaklı tüm özel şirketler de biz tüketicilere veya diğer şirket ve kurumlara sunmuş oldukları hizmet ve ürünler ile iletişimlerini sanal ortamlar üzerinden gerçekleştirmeye başladılar.

Sanal alem, siber alem gibi kavramlarla anlattığımız bu dünya üzerinde artık sanal ve gerçek mal varlıklarımızla üretmiş olduğumuz verilerle ve yaşantımızla yer alıyor. Diğer insanlarla kurduğumuz iletişiminin büyük bir kısmını elektronik ortamlarda gerçekleştiriyoruz. Bahsetmiş olduğumuz tüm bu sanal yaşam içerisinde **siber saldırganlara karşı** kendimizi ve kurumlarımızı korumak zorundayız. Bu noktada karşımıza "Siber Güvenlik" tanımı çıkıyor.

Siber kelimesi ise altyapısı bilişim sistemleri olan ağlara verilen addır. Genelde sanal gerçeklik şeklinde de tanımlanabilir. Kısaca Siber Güvenlik, alt yapısı bilişim sistemleri olan siber ağlar üzerinde yaşanan hayatın güvenliğinin sağlanması, bütünlüğünün ve gizliliğinin korunmasıdır.

Bilgi güvenliği ve **siber güvenlik** çoğu zaman birbirleri yerine kullanılan ancak birbirlerinden farklı olgulardır. Bilgi güvenliği bilginin bütünlüğünün, güvenliğinin ve gizliliğinin korunması olarak tanımlanır ve ISO 27001, ITIL, COBIT gibi global çapta kabul görmüş standartlarla sınırları çizilmiştir. Ancak alt yapısı bilişim sistemleri olan bilgi güvenliğini de kapsayan çok daha geniş bir kavramdır.

Kurumlar Açısından Siber Güvenlik Nedir? Veri Güvenliği

Kurumlar, şirketler ve kobiler penceresinden **siber güvenlik** kavramına baktığımız zaman karşımıza ilk olarak bilgi güvenliği kavramı gelmektedir. Kurumların sahip oldukları varlıkların en başında **"veri / bilgi"** gelmektedir. Kurumlar sahip oldukları bilgiyi derler, işler, satar, kiralar veya bir ürün / değer üretmek için kullanabilirler. Kurumlar için kritik önem arz eden bilgi güvenliği için global dünyada birçok standart oluşturulmuştur. ISO 2701 kurumlar için üretilen global çaptaki ilk ve tek denetlenebilir bilgi güvenliği standardıdır. **Bilgi güvenliğini sağlayarak gizli verilerini ve sahip oldukları en önemli varlığı, "bilgi"yi korumakla yükümlüdürler.**

Aksi takdirde siber saldırganlar, kötü niyetli hackerlar veya hacker grupları bu verilere izinsiz erişerek kurumlara maddi ve manevi olarak büyük zararlara sebep olabilirler.

Hackerler bilgisayar dünyasında genelde "üstat" olarak tanımlanan, bilişim sistemleri üzerinde uzmanlıklarını kanıtlamış iyi niyetli ürünlere, yazılımlara ve teknolojiye farklı pencerelerden bakarak zafiyetlerini keşfeden teknik beceri sahibi kişilerdir. İyi birer yazılım (kodlama) uzmanıdır ve teknolojiyi çok iyi kullanırlar. Ancak yazılı ve görsel basının sürekli olarak kötü niyetli hackerları ön plana çıkartması sebebi ile Hacker kelimesi kötü bir anlam kazanmıştır.

Bilişim sistemlerine sızan, zarar veren, bilgileri çalan veyahut illegal olarak dağıtan kişiler genelde Cracker, kötü niyetli Hacker veya bilgisayar korsanı şeklinde tanımlanırlar.

Hükümetler açısından siber güvenliğe baktığımız zaman akla ilk olarak vatandaşların, kamu kurumlarının, altyapısı bilişim sistemleri olan ve önem arz eden iletişim, finans, enerji gibi kritik altyapıların bilgisayar korsanlarına veya diğer devletlere karşı korunması gelir.

Genel olarak tanımlar birbirlerine benzer ancak önemli farklılıklarla ayrılsalar dahi, siber güvenlik olgusu bireylerin, kurumların veya hükumetlerin bilgi işlem sistemlerini güvenilir bir şekilde sürdürebilmesi sağlamak, siber saldırılara karşı ve izinsiz erişimlere karşı korunması olarak tanımlanır.

Siber Tehditler

• Bilgi güvenliğini ihlal edecek tüm faaliyetler
– DDoS saldırıları: internet üzerinden sistemlerin erişilebilir olmasını engelleme
– Hacking aktiviteleri
• Bilgi sızdırma faaliyetleri
–RSA
–Sony PS ağı üyelerinin bilgilerinin sızması
• Prestij zarar verme faaliyetleri
• Casus yazılımlar

Siber Ordu

• Ülkeyi, kurumu siber dünyadan gelebilecek tehlikelere karşı koruyacak ve gerektiğinde siber saldırılar gerçekleştirebilecek yetenekteki bilgi güvenliği uzmanlarının oluşturduğu ordudur.
• Siber ordu mensubu tüm askerler hem saldırı hem de koruma yöntemlerini çok iyi bilmek zorundadırlar .
• İki tür siber ordu bulunmaktadır:
– Devlet eliyle yetiştirilen resmi birimler
– Gönüllü fakat resmi ayağı olmayan birimler

Siber Savaş

• Bilişim sistemleri kullanılarak gerçekleştirilen ve amacı bir şirkete, bir ülkeye veya bir gruba yönelik maddi, manevi zararlar verme olan faaliyetler.
• 2010 Türkiye örneği:
– Yotube yasağını protesto eden bir grup Hacker Çeşitli bakanlık sitelerine yönelik DDoS saldırıları gerçekleştirdi.

Siber Savaş Tarafları

• Hacker grupları
• Ticari markalar, ticari firmalar
• Devletler

Siber Savaş Bileşenleri
• Fiziksel & sosyal bileşenler
– Hacker grupları
– “Gönüllü zombi” orduları
– Hükümetler ve askeri kurumlar
– İstihbarat servisleri
• Offensive & Defensive güvenlik yazılımları
– Nmap, Metasploit, Nessus, Snort, Packet Filter, özel amaçla geliştirilmiş yazılımlar
• Amaç & yöntem
– İnternet erişimi durdurma(availability)
– Bilgi sızdırma, ajan programlar yükleme

Siber Saldırı ve Tehditlere Karşı Savunma, Korunma Yöntem ve Sistemleri

Son zamanlarda teknolojide yaşanan gelişmeler ve internetin yaygınlaşması sonucunda kötü niyetli kişiler de bunlara paralel olarak, kullandıkları siber saldırı tekniklerini geliştirmiş, sistem ve teknolojilerin açıklıklarından daha fazla faydalanarak hedef sistemlere daha büyük zararlar vermeye başlamıştır. Hedef sistemlerin içerisinde, kurum, kuruluş veya ülkeler için hayati önemi haiz kritik altyapı sektörlerinin olduğunu düşünürsek, ortadaki zararın boyutunun ne kadar büyük olduğu anlaşılacaktır. Siber saldırı ve tehditlerin artması ve bunların sebep olduğu büyük mali

kayıplarla birlikte kamu düzeni ve güvenliğini etkileyerek tehlikeye sokacak noktaya gelmeleri sebebiyle siber saldırılara karşı topyekûn olarak bireyler, sivil toplum kuruluşları, kamu kurumları ve ulusal boyutta korunma yöntemleri geliştirilmeli ve uygulanmalıdır. Siber güvenliğin sağlanması konusunda ulusal boyutta yapılması gereken çalışmalar aşağıda belirtilen adımlardan oluşmaktadır:

1. Ulusal politika ve stratejinin geliştirilmesi: Siber güvenlik konusunda başarılı olunabilmesi için en başta bireyler, sivil toplum kuruluşları, kamu kurumlarına yol gösterici nitelikte bir ulusal politika ve stratejinin geliştirilmesi gerekmektedir

2. Yasal çerçevenin oluşturulması: Cana veya mala etki eden siber saldırı veya tehditlerin suç olarak tanımlanması ve cezalandırılması, özellikle siber saldırganların caydırılması konusunda büyük önem teşkil etmektedir. Bu bağlamda, yasal mevzuatın gelişen teknolojilere, siber saldırı araç ve yöntemlerine göre eksikliklerinin giderilmesi ve güncellenmesi gerekmektedir

3. Teknik tedbirlerin geliştirilmesi: Yasal çerçevenin oluşturulmasının yanında başta kişisel olmak üzere kamu kurum ve kuruluşların sahip oldukları bilgi ve iletişim teknolojilerinin yazılım ve donanım parçalarının da güvenliğinin sağlanması gerekmektedir. Bunun için de cihazların güvenlik standartlarının, teknik rehber ve kılavuzlarının geliştirilmesi, uygulanması ve kullanılması gerekmektedir.

4. Kurumsal yapılanmanın belirlenmesi: Bireyler, sivil toplum kuruluşları, özel sektör ve kamu kurum ve kuruluşlarının hepsinin görev ve sorumluğu olan siber güvenliğin başarıya ulaşabilmesi için asıl görevi ve vazifesi siber güvenlik olacak bir kamu kurumunun seçilerek, onun koordinatörlüğünde bilgisayar olaylarına müdahale ekibinin oluşturulması önem arz etmektedir. Bilgisayar olaylarına müdahale ekibi, bilgisayar güvenlik olaylarını tespit ederek, sorunları çözmek ve gelecekte olabilecek olayları önlemek için alınacak tedbirleri belirlerken internet kullanıcıları ile müşterek çalışan yapıya sahip aynı zamanda da bir koordinasyon merkezidir

5. Ulusal işbirliği ve koordinasyonun sağlanması: Farklı kurum, kuruluşlarca kullanılan sistemler, şebekeler ve altyapıların neredeyse tamamı birbirine bağlı ve bağımlı olmakla birlikte sadece birindeki zafiyet veya açıklık tüm sisteme zarar vermektedir. Topyekûn bir güvenliğin sağlanabilmesi için ise tüm kurum ve kuruluşlar arası sıkı bir işbirliği ve koordinasyon sağlanmalıdır.

6. Kapasitenin geliştirilmesi: Teknolojide yaşanan gelişmeler, siber saldırı ve tehditlerin araç ve yöntemlerini de değiştirmiş ve geliştirmiştir. Buna karşılık, sistemlerin güvenliğini sağlama konusunda uygulanacak politikalar, yasalar, standartlar, ürünler ve çözümler de bu değişim ve gelişime uygun olarak oluşturulmalıdır. Bu sebeple politika belirleyiciler, hukukçular, yazılım, donanım ve uygulama geliştiriciler, kolluk görevlileri de teknik ve idari kapasitelerini geliştirmelidir (Ünver ve Canbay, 2010: 99).

7. Farkındalık Oluşturma: Eğitim kuruluşları ve kitle iletişim araçları kullanılarak, son kullanıcılara kadar kişiler, değişen siber saldırı araç ve yöntemleri konusunda bilgilendirilmeli, farkındalık ve bilgi düzeyleri yükseltilmelidir. Siber saldırılara karşı oluşturulmuş olan güvenlik politikalarının kullanıcılar tarafından içselleştirilerek bu anlamda bir kültürün oluşturulması çok önem arz etmektedir (Tombul, 2015: 163; Ünver ve Canbay, 2010: 99).

8. Uluslararası işbirliği ve uyumun sağlanması: Günümüzde bireysel, kurumsal ve ulusal tüm altyapı ve sistemler küresel bir ağ olan internet üzerinden birbirlerine bağlı ve bağımlıdır. Bu ağın güvenliği ise ancak uluslararası işbirliği ve koordinasyon ile sağlanabilir. Bu işbirliği çerçevesinde ortak bir mevzuatın oluşturulması, suç soruşturma ve kovuşturma usul ve yöntemlerinin uyumlu hale getirilerek, bilgi paylaşım mekanizmalarının oluşturulması gerekmektedir.

SİBER SALDIRI TÜRLERİ

4.1. Sniffing

Sniffing temel olarak verinin yolunu kesmek olarak tabir edilebilir. Sniffing ile networkdeki paketler yakalanabilir içeriği okunabilir. Kelime anlamı koklamak olan sniffing, bir ağ üzerindeki bilgisayarlar arasındaki veri trafiğinin dinlenmesi anlamına gelmektedir. Bunu yapmak için internette bol miktarda yazılım bulunmaktadır. Şebeke trafiğinin dinlenmesinde mantık, yönlendiricilere gelen h e r paketin kabul edilmesi dolayısıyla iki bilgisayar arasındaki tüm verilerin yakalanarak saklanmasıdır. Bu, korsanların kullandığı en önemli yöntemlerden birisidir. Bu yöntemden korunmak için bilgisayarlar arasındaki bağlantıların şifreli olması gerekmektedir. Kriptolu paketler de elbette dinlenip ele geçecektir ancak içeriğinden bir şey anlaşılamayacaktır. (BGA, 2012)

Sniffingin amacı; Şifreleri (email, web, ftp, telnet, SQL, Email text'ini Transfer edilen dosyaları (e-mail, ftp) yakalamaktır.

4.2. Hizmet Dışı Bırakma (Denial Of Service)

DoS(Denial of Service), hizmeti aksatma veya hizmetin işlevini tamamen yok etme anlamına gelmektedir. İnternet kullanıcılarına ya hiç hizmet veremez ya da çok yavaş bir hizmet sunar.

DDos(Distrubuted Denial of Service) saldırısı ise, saldırganın saldırıya geçmeden önce oluşturduğu makine veya bilgisayar topluluğu ile hedefe saldırmasıdır ve DoS gibi hizmet aksatma veya hiç hizmet veremez hale getirme amaçlanır. Bununla birlikte saldırgan kolay bir şekilde kimliğini belli etmeden gizlenebilir ve saldırganın tespit edilmesi zorlaşır. DoS saldırı türünde amaç sınırlı sistem kaynaklarının sınırını aşarak, sistemin devre dışı kalmasını sağlamaktadır.

olarak SYN+ACK paketlerini yollar ve ACK paketini beklemeye koyulur. Buraya kadar herşey güzel. ACK paketi gelmez ise bu bağlantı full -duplex değil "yarı-açık" bir bağlantı olurdu ve bu bağlantı çeşidi pek iç açıcı değildir.

Sunucu SYN+ACK'yi yolladıktan sonar ACK için bekler. Fakat istemci ACK paketini yollamaz ise işler çıkmaza girer. Sunucu beklemeyi bırakmaz sürekli bekler.

Sunucu ACK için beklerken, karşıya ACK yerine bir bağlantı talebinde daha bulunduğumuzu varsayalım. Ve yine 3. adım'ı gerçekleştirmeyelim. Yani son ACK'yi yollamayalım. Hatta bunun tekrar tekrar yapılması ile sonuçta "flood" oluşur.

Hedef makine, saldırı yapılan makineden yanıt alamayacağından dolayı, SYN-ACK paketini 5 kez tekrar edecektir. Bunun tekrar süreleri, 3, 6, 12, 24 ve 48 saniyedir. Ayırdığı kaynağı boşa çıkartmadan evvel, 96 saniye sonra son bir kez SYN-ACK denemesi yapacaktır. Hepsini topladığınızda, görüldüğü gibi hedef makine ayırdığı kaynakları 3 dakika gibi bir süre tutacaktır. Bu sadece her bir SYN atağı için gerçekleşecek süredir.

Saldırı DoS saldırısı olursa, yani tek bir IP üzerinden saldırı gerçekleşirse firewall'dan engellenebilir. Fakat DDoS saldırısında çok sayıda makine kullanıldığından, ip tespiti güçleşir ve firewall yakalayamayabilir. Log taşması sonucu firewall devre dışı kalabilmektedir. Bu nedenle DDoS, DoS saldırısına göre daha tehlikeli ve etkilidir. DoS saldırıları siber tehditler arasında 2. Sıraya girebilmektedir.

DRDoS, yani "Distrubuted Reflective Denial Of Service" DDoS'a benzerdir. Tek farkı, daha sık aralıklarla atak yapmak amacıyla ek ağlar kullanmaktadır.

4.2.1. DoS saldırı çeşitleri

TCP three handshake tamamlanmadan yapılan bir yöntemdir. Yani istemci bir SYN, sunucuda buna yanıt

Saldırgan bu tekniği tekrarlanan bir şekilde gerçekleştirdiği zaman, hedef makine ayırdığı kaynaklardan dolayı kaynak yetersizliğine kadar ulaşır ve artık yeni bir bağlantı karşılayamayacak duruma gelir. Ve bu durumda yetkili kullanıcılar bile makineye bağlanamaz. Yetkililer ne kadar bağlantı iptal ederlerse etsinler, yenileri eklenecektir.

TCP-SYN oturumu host ile client arasında kurulduktan sonra ACK veya PUSH ACK paketleri iletişim için kullanılır. Bu ACK paketleri kurban server' in kaynaklarını tüketmeye başlarsa ACK & PUSH ACK Flood olarak adlandırılan atak gerçekleşmiş olur.

Eğer atak türü kurban nerwork'un bank genişliğini sömürürse, buna ACK & PUSH ACK Flood türü olan Fragmented ACK denir. Atak'da 1500 byte uzunluğunda paketler kullanılır.

TCP-SYN oturumunu sonlandırmak için RST veya FIN(açık olan TCP iletişim handshake oturumunu sonlandırma isteği) server değiştirir. RST veya FIN atak esnasında, kurban server RST veya FIN paketlerini yüksek oranda kaydeder ve sonuç olarak server'in kaynakları tükenmeye başlar (hafıza, CPU, RAM, vb.). Bu da RST veya FIN Flood olarak bilinir. Server bunu karşılayamazsa performansı azalır, isteklere cevap veremez veya kapanır.

4.3. IP Aldatması (IP Spoofing)

Bilgisayarlar arasındaki bağlantı çeşitli protokoller aracılığıyla sağlanmaktadır. Bu protokoller aracılığıyla başka bir bilgisayara bağlanıldığında bağlanan bilgisayar kendi kimliğini karşı tarafa tanıtır. Bağlanılan bir bilgisayara gerçek IP adresinin gösterilmemesi yani asıl kimliğin gizlenmesine IP spoofing (Aldatma) denir.

Sahte IP paketi alan bilgisayar, paketin gerçekten gönderilen adresten gelip gelmediğini bilemez. Bu genellikle başkasının IP adresinden mail gönderilmesi veya forumlara mesaj yazılması olarak karşımıza çıkmaktadır. Teoride bu durum mümkün olmakla birlikte pratikte karşıdaki sistem gerçekten ele geçirilmeden başkasının bilgisayarına farklı bir IP'den bağlanma gerçekleşemeyecektir. Günümüzde IP spoofing için kullanılan ticari ve ücretsiz yazılımlar bulunmaktadır. (Lewis & Timlin, 2011)

Aldatma genel olarak bir web sitesini işlemez hale getirmek için saldırı esnasında kaynağı gizleme maksadıyla kullanılmaktadır.

Aldatma genel olarak bir web sitesini işlemez hale

getirmek için saldırı esnasında kaynağı gizleme maksadıyla kullanılmaktadır.

4.3.1. Spoofing'den korunma yöntemleri

IP Spoofing olayını engelleyebilmek için öncelikli olarak yönlendiricilerde, kaynak yönlendirme fonksiyonunu pasife alınmalıdır. Çünkü kaynak yönlendirme çok kısıtlı ve

pek nadir kullanılır. Bu nedenle ağa giren ve çıkan bu trafik engellenmelidir. Sisteminizde filtre uygulanmalı ve yetkiler kısıtlanmalıdır. Şöyle ki; sistemde IP adreslerini değiştirme hakkı kaldırılmalıdır. Dolayısıyla (IP) Spoofing'in önüne geçilebilir. Bunlara ek olarak bir takım yazılımları kullanabilirsiniz. Bu yazılımlar Spoofing yapılırken uygulanan metotlara rastladığı zaman size haber verir.

4.4. Sosyal Mühendislik

Sosyal Mühendislik; temel olarak bilgisayar ya da bilgisayar ağlarındaki açıklıklardan faydalanarak bilgisayar sistemlerine zarar veren yaklaşımların aksine "sosyal mühendislik" yöntemi insanların iletişim, düşünce tarzı, güven ya da kısaca insani zaaflarından faydalanarak siber güvenlik süreçlerinin etkisiz hale getirilmesi ya da atlatılması şeklinde tanımlanabilir. Sosyal mühendislik yöntemleri; çeşitli yalanlar yolu ile sahte senaryolar üretmek, hedef kişiye kendini güvenilir bir kaynak olarak tanıtmak ya da basit ödüllendirme yöntemleri ile bilgi sızdırmak şeklinde özetlenebilir. (i n t e r n e t , 2 0 1 0)

4.5. SQL Enjeksiyonu

SQL enjeksiyonu veri tabanından yapılan sorgulama işlemini hedef alan bir saldırı şeklidir. Bu saldırı şeklinde sorgulama dili yapısı kullanılarak saldırı gerçekleştirilir. Bir web uygulamasının kullanıcı adı ve şifre ikilisi veri tabanına "SELECT * FROM TABLE_ PERSONEL WHERE username = '" + kullanıcı adı + "' AND password= '" +şifre+ "'" şeklinde gönderildiğinde (" ") işaretleri içindeki veri bir filtrelemeye tabi tutulmazsa kullanıcının buraya yazacağı (OR ''1=) eklinde bir ifade sorguyu "SELECT * FROM TABLE_PERSONEL

WHERE username = '' OR ''1=1'' AND Password = '' OR ''1=1'"" haline getirir. Bu durumda sorgudan var olan bütün kayıtlar dönecektir. (Hughes, 2009)

4.5.1. Komut enjeksiyonu

Genellikle komut (shell) enjeksiyon saldırılar SQL enjeksiyon ve XSS saldırılarının aksine doğrudan sunucuları hedefleyen bir saldırı tipidir. Web uygulamasının komut satırını kullanarak uzaktan erişimle işletim sistemi, veri tabanı yönetim sistemi ve sunucudaki bilgilere erişimi hedefler. (Rapor, 2012)

4.5.2. HTML enjeksiyonu

Bu açık, programcıların kodlama sırasında yaptığı hatalı kodlamadan faydalanır. Web yazılımlarında veri tabanına giren verilerin ya da veri tabanından çekilen verilerin bir kontrol mekanizmasından geçirilmemesi açığa neden olmaktadır. XSS olarak da bilinen açıktan faydalanılarak session ve cookie çalması yapılır. Uygulamalarda sayfaya gönderilen bir isteğe bir cevap döndürülmesi mantığı kullanılır. Sayfaya gönderilen istek sunucuda değerlendirilip bir cevap döndürülür. Ama eğer giriş yaptığınız sayfa kötü amaçlı bir url adresine yönlendirildiyse ya da Truva atı gibi araçlar yerleştirildiyse aldığınız yanıt beklenenden farklı olacaktır. Bu saldırı tipinde amaç web uygulamasına zarar vermek değil daha çok uygulamayı ziyaret eden kullanıcılara erişmektir. (TCK, 2013)

4.6. Arka Kapılar (Backdoors)

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 portu açık tutmaktır.

Bu açıdan bakıldığında bu tür bir açığa maruz kalındığından emin olmak için sistemde mevcut bulunan bütün portlar 1'den 65535'e kadar iki kere (bir kez TCP bir kez de UDP için) taranmalıdır. Arka kapılar çoğunlukla Truva atları ile karıştırılabilmektedirler. Her

ikisi de hedef sisteme sızmaya yarayan kötü amaçlı yazılımlardan; Truva atı faydalı bir program gibi gözükürken; arka kapı sadece sisteme erişimi sağlayan gizli yapılardır. (V., H., B., & G., 2013)

Birçok virüs bir bilgisayara bulaştığında mutlaka bir arka kapı açmayı denemektedir. Bu arka kapılar da virüs yayıncısı için çok kolay bir erişim imkânı sağlamaktadır. Arka kapılar kimi zaman sistemi geliştiren programcı tarafından test edilen sisteme erişmek amacıyla kullanılan fakat daha sonra unutulan açıklar olarak karşımıza çıkmaktadır. Bu durumun bir şekilde farkına

varan kötü niyetli kişiler bu yapıları kullanabilirler. Hatta bu tip arka kapılar bazen programcı tarafından kasten bırakılabilmektedir.

Arka kapı konusunda en ünlü iddialardan biri de Microsoft'un Windows işletim sisteminin bütün sürümlerinde NSA (Amerikan National Security Agency) için bir arka kapı yerleştirdiği iddiasıdır. Bu iddia Microsoft'un bütün sürümlerinde bulunan CryptoAPI yapısında _NSAKey adına ilave bir giriş anahtarın bulunmasıdır. (N., H., & Ö., 2013)

4.7. Oltalama (Phishing)

Phishing kısaca online dolandırıcılık olarak tanımlanabilir. Phishing yönteminde temel amaç internet kullanıcısını kandırarak kullanıcıya ilişkin kredi kartı bilgileri, banka hesap numaralarından, bu hesaba ait online internet şifresine kadar birçok özel bilgileri ele geçirmektir.

4.7.1. Neler çalınıyor?

Phishing yöntemi kullanarak bilgisayar kullanıcılarını tuzaklarına düşüren dolandırıcılar özellikle aşağıda belirtilen bilgileri çalıyorlar:

Kredi Debit/ATM Kart Numaraları/CVV2 Şifreler ve parolalar

Hesap numaraları

İnternet bankacılığına girişte kullanılan kullanıcı kodu ve şifreleri

4.8. Casus Yazılım (Spyware) Bu programlar kullanımı masum görünen ve genelde internetten "bedava" diye reklamını görüp indirilen programlar ile bilgisayarlara bulaşan programcıklardır.Çoğunlukla dikkat edilmeyen EULA (Son Kullanıcı Lisans Sözleşmesi) içerisinde (programla birlikte kurulacağı belirtilir ve "I Agree" kabul edildiğinde her şeyi kabul edilmiş olunuyor) bulunur. Tam anlamı ile virüs olarak adlandırılamayan bu programların temel amaçları kuruldukları bilgisayarda bilgi toplamak ve bu bilgileri bu programları yaratan kişilere göndermektir. Bu spyware/casus programların bilgisayar sistemlerine tehlikesi casusluk derecelerine göre değişir. Casusluk yaptıkları konular nispeten masum olarak adlandırılabilecek olan "hangi siteye gidiyor, ne kadar orada kalıyor" gibi bilgilerden daha ciddi olan bilgisayarın veya sistemin kurulum şifreleri veya kullanılan kredi kartı bilgilerini edinerek bunları program yazıcılarına postalamaya kadar varabilen her türlü casusluk örneklerini kapsayabilirler. Sörf bilgilerini genelde google toolbar, alexa toolbar veya diğer benzeri toolbar ismiyle dağıtılan internet explorer eklentileri biriktirirler. Bu şekilde hangi sitelerin ziyaret edildiğini ölçerek ziyaret edilen sitelere puan veya benzeri değerlendirmeler verirler. Sonra bu verileri arama sitelerinde sonuçları sıralamak için kullanabilirler. Aynı şekilde GetRight, Gator ve benzeri internetten dosya indirmeye yarayan programlar da bu tür spyware içerirler. Ancak bunu kendileri tabiî ki kabul etmezler çünkü bu programları kurarken kabul ettiğiniz kullanım kurallarına göre bu veri aktarımını kabul ettiğinizi bildirdiğiniz için bunun casusluk olmadığını gönüllü veri paylaşımı olduğunu belirtirler. Spyware veya casus programların daha tehlikeli olan türevleri ise bilgisayar veya internet ayarlarınızı kendi istedikleri gibi değiştirirler ve kendi istedikleri sitelere yönlendirirler bazıları bununla da yetinmeyip internet başlangıç sayfasını kendi istedikleri gibi değiştirirler hatta bazen bilgisayarda karşınıza nereden geldiğini bilmediğiniz ve anlayamadığınız reklam içerikli pencereler çıkarırlar. Bunlara Adware'de denir çünkü her ne kadar bir önceki casus programlar gibi casusluk yapıyor olsalar da bunun yanında ayrıca bir de bilgisayarınızda reklama yönelik oynamalar yapmaktadırlar. (Bakanlığı, 2013)

4.9. Virüsler

Virüs, bilgisayar dünyasında on yıllardır karşılaşılan bir terimdir. Bu terim genellikle zararlı yazılımları ifade eden kapsayıcı genel bir ifade olarak kullanılmıştır, ancak bu

kullanım yanlıştır. Her tür zararlı yazılım virüs olarak ifade edilemez. Virüs diğer dosyalara bulaşarak yayılan özel bir zararlı yazılım türünü ifade etmektedir. (Graham & Howard, 2010) Kayıtlara geçen ilk virüs 1986 yılında ortaya çıkan IBM-PC tabanlı "Brain " ismi verilen bir boot sector virüsüdür. (Graham & Howard, 2010)

Bir sistemdeki olası virüs belirtileri şunlardır:

İnternette bir işlem ya da faaliyet yapılmayan zamanlarda veri trafiğinin devam etmesi: Buna göre başka kişi veya kullanıcılar sistemde aktif olabilirler ve kötü niyetli bir çalışma yapıyor olabilirler.

Sistemde yapılandırılmış bir güvenlik duvarı olduğu takdirde bazı uygulamaların internetten bağlanma girişimleri.

İnternet sitelerinde dolaşırken reklam pencerelerinin açılması.

Bilgisayarın işlemez hale gelmesi.

Telefonlardaki kötü amaçlı yazılımlar.

4.10. Truva Atları

Faydalı bir fonksiyonu varmış gibi görünen fakat aynı zamanda gizli ve güvenlik mekanizmalarını aşabilecek potansiyel zararlı fonksiyon içeren ve bazen bir sistem biriminin meşru olarak yetkilendirilmesini istismar eden bir bilgisayar programı olarak tanımlanmaktadır. (Kissel, 2012).

Truva atları, bilgisayarları uzaktan yönetmek için arka kapı açan programlardır. Lisanslı programların yasa dışı kopyalarının veya aktivasyon kodlarının dagıtıldıgı "warez" diye adlandırılan siteleri veya bedava mp3, oyun veya yetişkin içerik dagıtan siteleri ziyaret eden kullanıcılar, farkında olmadan yukarıda belirtilen programları bilgisayarlarına

indirirken, aynı zamanda kötü niyetli programları da indirmiş olurlar. Bilgisayara kurulan bu programlar, arka plandan çalışarak, kullanıcının sistemine uzaktan erişim imkanı saglar. Truva atlarıyla sisteme arka kapıdan ulaşan bilgisayar korsanları, bilgisayarın sistem yapılanmasını degiştirebilir, kullanıcının şifrelerine ve diger kişisel bilgilerine ulaşma imkanına sahip olabilirler. Yani truva atı sisteme bulaştıktan sonra, sistemin açılmasıyla beraber kendisini belleğe yükler ve sistem ağlarının açıklarını kullanarak, programı yerleştiren taraf olan bilgisayar korsanının isteklerini yerine getirir. (Değirmenci, 2002)

Çeşitli truva atları mevcuttur. Bunların hepsi aynı amaca hizmet etmekle beraber, özellikleri bakımından birbirinden ayrılmaktadırlar. Truva atları altı grupta tasnif edilebilir. Bunlar; "uzaktan kontrol edilen truva atları", "parola truva atları", "imtiyazlı yükselen truva

atları", "anahtar kırıcı", "yıkıcı truva atları", ve "şaka programları"dır (Nagpal, 2005).

Bir truva atıyla bilgisayar korsanının yapabilecekleri, o truva atının program yapısına göre degişiklik arz etmektedir. Örnegin Back Office 2000 isimli truva atı programı ile;

CD-ROM sürücüsü açılıp kapatılabilir,

Sistem ekranına çeşitli mesajlar gönderilebilir, Sistem kapatılabilir,

Sabit diskteki istediginiz dosyalar silinebilir,

Bilgisayar korsanı, sabit diskten kendi bilgisayarına dosya transfer edebilir veya müdahale edilen

bilgisayara istedigi bir dosyayı yerleştirilebilir, Giriş şifresi, kredi kartı şifresi gibi önemli bilgiler ele geçirilebilir (Değirmenci, 2002) .

4.11. Solucanlar (Worms)

Solucanlar da, tıpkı virüslerde olduğu gibi, kendini bir cihazdan başkasına kopyalamak üzere tasarlanmışlardır, ancak bunu kendi başlarına gerçekleştirmektedirler. Öncelikle bilgisayarda dosya veya veri transferi yapan fonksiyonların denetimini ellerine geçirip bir kez sisteme bulaştıktan sonra kendi kendine yollarına devam edebilirler. Solucanların en göze batan tehlikesi, büyük miktarlarda çoğalma yetenekleridir. Kullanıcıların veri ve dosya alışveriş yöntemlerini kullanarak kendilerini, irtibat halinde olunan tüm bilgisayarlara, tüm e-posta adreslerine gönderebilmektedirler. Bu da ağ trafiğinin önemli derecede yavaşlamasına neden olabilmektedir. Bir solucan yeni çıktığında, daha güvenlik yazılımları tarafından tanınmadığı için ilk etapta ağ trafiğini önemli oranda yavaşlatabilmektedir. Karıştırılan terimler oldukları için virüsleri, Truva atları ve solucanlardan ayıran özelliği burada vurgulamakta fayda bulunmaktadır: Truva atları zararsız birer yazılım gibi görünmekte ve bir sistemde istismar edeceği bir durum ortaya çıktığında (bilgisayarın İnternete bağlanması gibi) devreye girmekte, diğer zamanlarda sisteme herhangi bir müdahalede bulunmamaktadır. Solucanlar ise ağda kendilerini yayabilen kendi başlarına birer programdırlar. Bunların aksine virüs, bulaşmak için kendine yeten bir program değildir. Kendini başka dosyalara ilave ederek yayılır ve eğer virüslü dosya açılmazsa virüs başka ortamlara yayılamaz.

Tübitak tarafından 2011 yılında yapılan bir açıklamada son yılların en büyük saldırılarından biri olan ve tüm dünyada 15 milyon bilgisayara bulaştığı tahmin edilen "Conficker" adlı solucanın zayıf şifrelere sahip kullanıcı hesapları aracılığıyla ağ üzerindeki paylaşımlarla ve solucanın bulaştığı bilgisayarlara takılan taşınabilir bellekler vasıtasıyla yayıldığı belirtilmiştir.

4.12. Bot

Bot bilişim dünyasında "robot" anlamında kullanılan yaygın bir terimdir. Pek çok bilgisayar işlemini yarı otomatik olarak yapabilen robotlar bilişimin tüm alanlarında

kullanılır. En ünlü oldukları alan arama motorları tarafından kullanıldıkları endeksleme teknolojisidir. Akıllı ajan teknolojilerinin internet ile birlikte hızla yaygınlaşması internet robotu ya da kısaca bot olarak adlandırılan ve özel olarak internet üzerinde hareket göstermek üzere geliştirilen bir ajan yazılımı grubunu ortaya çıkarmıştır. Bu grupta esasen web tabanlı arama motorlarının çekirdeklerinde yer alan örümcek yazılımları ve özel amaçlı tarayıcı yazılımlar gibi değişik türler de yer alır. Kesin bir çizgi olmamakla birlikte Çek dilinde iş anlamına gelen robota kelimesinden türeyen robot kelimesinin kısaltılmışı olan bot kavramı akıllı ajan yazılımlarının İnternet üzerinde etkinlik gösterenlerine verilen bir ad olmuştur. Belki de bu adlandırmada gerçek dünyada robot davranışı olarak adlandırılabilecek türden davranışların sanal dünyadaki karşılığı olmaları beklentisi etkili olmuştur.

Günümüzde pek çok değişik bot türünden söz edilmektedir. Ticari veri madenciliği, e-posta, oyun, kamusal haber grubu, sohbet, alışveriş, hisse senedi, yazılım vb. gibi hedeflenen bilgi türüne göre adlandırılan pek çok bot türü mevcuttur. Bu türlerin hemen hepsi karakteristik olarak otonom bilgi ajanları/arabirimleri olarak ve özellikle internet üzerinde faaliyet göstermek üzere tasarlanmış ve geliştirilmiş yazılım türleridir.

4.13. Zombi Ordular (Botnetler)

Zombi bilgisayarlar ya da botnetler bu tehdit grubunun en tehlikeli olanları olarak kabul edilebilir. Burada önemli olan nokta, bilgisayar kullanıcısının hiçbir haberi olmaksızın bilgisayarının çok ciddi suçlar işlenmesinde kullanılabilmesidir. Bu tür bilgisayarlar robot veya bot şeklinde de ifade edilmektedir. Zombi ordunun bir parçası haline gelen bilgisayarlarda buna sebep olan nokta, genellikle bu tür bilgisayarların firewall denilen güvenlik duvarlarının olmamasıdır. Günümüzde bant genişliğinin artmasıyla beraber herhangi bir korunmaya sahip olmayan bir bilgisayar kolaylıkla bir botnet'in parçası haline gelebilir. Bir botnet, genellikle açık bırakılan bir kapıdan (port) bir bilgisayara, daha sonra aktif hale gelecek şekilde, Truva atı bırakılması sonucu oluşturulmaktadır. Botnet'in parçası haline gelen bilgisayarlar mesela bir web sitesine aynı anda yönlendirilerek bu siteyi hizmet veremez hale getirmek için kullanılabilmektedir. (SearchSecurity, 2012)

4.14. Bukalemun

Normal bir program gibi çalışan "bukalemun", aslında bir takım hile ve aldatmalar uygulayarak çok kullanıcılı sistemlerde kullanıcı adları ve şifrelerini taklit yeteneği sayesinde gizli bir dosyaya kaydederek, sistemin bakımı için geçici bir süre kapatılacağına ilişkin bi (YerTutucu1)r uyarı verir. Bu sırada bukalemun programını kullanan kişi, bu gizli dosyaya ulaşarak kullanıcı adlarını ve şifrelerini ele geçirir (Aydın, 1992).

4.15. Klavye İşlemlerini Kaydeden Programlar (Keyloggers)

Keylogger'lar kısaca klavye işlemlerini kaydeden programcıklardır. Bu programcıklar, farkına varılmadan klavyede dokunulan her tuşu kaydedip, fırsatını bulduklarında daha önce belirlenen adreslere bunları göndermektedirler. Özellikle bankacılık işlemlerinde klavyeden şifre girilmemesi, rakamlara tıklanarak veya rakamların üzerlerinde beklenerek şifreler girilmesi ve ayrıca cep telefonu ile SMS şifreleri yoluyla ilave güvenlik desteği sunulabilmesine rağmen internet üzerinden ticaret yapan birçok site, alıcıların kredi kartı bilgilerini girmesi için güvenlik seviyesi yüksek bu tür platformlar oluşturmamaktadır. Bu da klavyeden girilen bu bilgilerin nasıl kolayca başkalarının eline geçebileceğini göstermektedir. Bu durum, sadece alışveriş ve bankacılık işlemleriyle sınırlı değildir. Klavye işlemlerini kaydeden bu tür yazılımlar nedeniyle, e-posta ve sosyal paylaşım siteleri gibi kullanıcıların özel bilgilerinin yer aldığı web sitelerine ait kullanıcı adları ve şifrelerin ne kadar büyük tehlike altında olduğu anlaşılabilmektedir. Günümüzde sosyal medya ve çevrimiçi (online) oyunların ne kadar yaygın olduğu ve bunlar yüzünden meydana gelen cinayet ve intiharların ne kadar çok arttığı göz önünde bulundurulursa keylogger'ların meydana getirdiği asıl tehlike gerçek manasıyla anlaşılabilir.

Bu yazılımlar, aynı zamanda aldatan bir eşi takip etmede, işverenlerin çalışanlarını izlemesinde veya bir çocuğun bilgisayarda neler yaptığının gözlenmesinde kullanılabilmektedir. Bu programlar, maksatlı kişiler tarafından bilgisayarlara doğrudan fiziksel erişim sağlanarak veya İnternete bağlı olan bir bilgisayardaki açıklıklar kullanılarak sistemlerin içerisine kurulabilir. (Subramanyam & Frank, 2012)

Keylogger'lar küçük programcıklardır ancak bunlar sadece yazılım olarak değil donanım olarak da var olabilmektedirler ve kullanıcılar ve sistemler bunların farkına

varamamaktadırlar. Bu tür klavye hareketlerini kaydeden donanımlar fiziksel olarak klavye ile bilgisayar arasına monte edilmekte ve bilgisayar kasasının arka kısmına gizlenmektedir. Yapılan araştırmalarda ne kullanıcılar, ne de sistemler bu kaydedicileri fark etmiştir. Hazırlanmaları ve kurulumları çok basit olan bu tür cihaz ve yazılımların varlıklarına karşı dikkatli olunması gerekmektedi (YerTutucu1)r. (Subramanyam & Frank, 2012)