Siber Güvenlik Terimleri Sözlüğü Bu sözlük, siber güvenlikle ilgili olarak seçilen terimleri içerir.
Gelişmiş Sürekli Tehdit (APT): Çok sayıda aşamadan oluşan ve uzun süreli bir ağ saldırısıdır ve bu saldırı türünde, yetkisiz kullanıcılar değerli kurumsal verilere erişir ve bunları toplar.
Kimlik Doğrulaması: Bir bilgisayar sisteminin kullanıcısının gerçekten olduğunu iddia ettiği kişi olduğunun kanıtını sunan bir güvenlik hizmetidir.
Yedekleme: Bir bilgisayarın ele geçirilmesi halinde tüm önemli verilerin kaybolmasının önlenmesi için verilerin güvenli bir uzak konumda depolanmasını sağlar.
Botnet: Potansiyel olarak dünyanın herhangi bir yerinde bulunan, bir kötü amaçlı yazılım parçasının bulaşmış olduğu bir grup bilgisayar sistemidir. Yazılım, bulaştığı bilgisayarların bir bilgisayar korsanı tarafından bir ağ haline getirilmesine olanak sağlar. Bilgisayar korsanı, ağ üzerindeki tüm botların tam kontrolünü elde eder ve kötü amaçlı görevleri yerine getirebilir.
İhlal: Yetkisiz bir kullanıcının ya da yetkisiz erişen bir kişinin (bilgisayar korsanı) bir bilgisayardaki ya da aygıttaki bir güvenlik açığını başarıyla istismar ettiği ve dosyaları ile ağına erişim elde ettiği andır.
Kaba Kuvvet Saldırısı: Bir bilgisayar korsanının, örneğin parolasını "tahmin etmeye" çalışarak bir bilgisayar sistemine yetkisiz olarak erişmek için kullanabileceği bir yöntemdir.
Bulut: Yüksek depolama kapasitesine sahip olan ve müşteri dosyası taleplerine uzaktan hizmet sunan bir dizi bilgisayardır; teknoloji, dosyalara İnternet üzerinden, dünyanın herhangi bir yerinden erişilmesine olanak sağlar.
Komuta ve Kontrol Merkezi: Bir botnetteki tüm botları kontrol eden bir uygulamadır. Bir bilgisayar korsanı, bir uygulama aracılığıyla bir komut gönderir ve bu uygulama daha sonra komutu bir ağ üzerindeki tüm ele geçirilmiş bilgisayarlara aktarır.
Siber Saldırı: Siber yöntemler aracılığıyla bilgisayar sistemlerine, ağlara veya aygıtlara zarar verilmesine, bunlarda aksaklık oluşturulmasına veya bunlara yetkisiz erişim elde edilmesine yönelik kötü amaçlı girişimlerdir.
Siber Güvenlik: Bilgilerin siber uzaydaki gizliliğinin, bütünlüğünün ve kullanılabilirliğinin korunmasıdır.
Dijital İmza: Bir özel anahtar ile şifrelenmiş ve mesajın ya da nesnenin orijinalliğinin ve bütünlüğünün alıcıya garanti edilmesi için bir mesaja ya da nesneye eklenmiş olan bilgilerdir.
Dijital İmza: Bir özel anahtar ile şifrelenmiş ve mesajın ya da nesnenin orijinalliğinin ve bütünlüğünün alıcıya garanti edilmesi için bir mesaja ya da nesneye eklenmiş olan bilgilerdir.

Şifreleme: Bir dosyanın içeriğini, iletişim zincirinin dışındakiler için okunamaz bir şeye dönüştüren algoritmik bir yöntemdir.
İstismar: Bir bilgisayarın güvenlik açığından yararlanmak amacıyla kullanılabilecek kötü amaçlı bir uygulama veya komut dosyasıdır.
Güvenlik Duvarı: Yetkisiz erişimin engellenmesine odaklanan donanım veya yazılım tabanlı bir savunma teknolojisidir. Bir kullanıcının bilgisayarı ve İnternet bağlantısı ile olan her etkileşim girişimini değerlendiren ve "buna izin verilmesinin uygun olup olmadığını" belirleyen bir ”duvar” ya da filtre oluşturulur.
Bal Çanağı (honeypot): Savunma amaçlı bir siber güvenlik yöntemidir. Bu yöntem, bir ağ üzerinde yasal ve yüksek değerli bir hedef gibi görünecek şekilde tasarlanmış bir bilgisayarın (sunucu) kullanılmasını kapsar. Amaç, bilgisayar korsanlarının gerçekten yüksek değerli olan bilgisayarlar veya veriler yerine bu bilgisayara odaklanmasının sağlanmasıdır. Bal çanağı yöntemi, sistem yöneticilerinin bilgisayar korsanlarını "iş başında" izlemelerine ve saldırı yöntemlerinden nasıl korunacaklarını öğrenmelerine olanak sağlar.
İç Tehdit: Bir kuruluşun karşı karşıya olduğu ve kuruluşun güvenlik uygulamalarına, verilerine ve bilgisayar sistemlerine ilişkin olarak "içeriden bilgi sahibi olan" mevcut ve eski çalışanları, yüklenicileri veya iş ortakları gibi kişilerden kaynaklanan kötü amaçlı bir tehdittir.
Jailbreak: Bir aygıt üzerindeki yazılım kısıtlamaları atlanarak bir kullanıcının bir işletim sistemine ya da çekirdeğe kök erişimi elde etmesidir. Bu yöntem, genellikle cep telefonu güvenliği bağlamında kullanılır.
Kötü Amaçlı Yazılım: Bir bilgisayarda karmaşaya neden olmak amacıyla tasarlanmış her tür kötü amaçlı yazılımı ifade eden genel bir terimdir. Tipik kötü amaçlı yazılım (malware) türleri arasında virüsler, Truva Atları, solucanlar ve fidye yazılımları yer alır.
Ortadaki Adam (MitM): Bir saldırganın, işlemleri gözlemek ve kaydetmek amacıyla bir kullanıcı ile web sitesi arasındaki mesajları yakaladığı izinsiz giriş yöntemidir. MitM saldırıları, kimlik avı dolandırıcılığı ile site trafiğini yönlendirme saldırılarının gelişmiş türevleridir. Bir MitM saldırısında, bir web sitesinde oturum açmış olan bir kullanıcı, kendisi ile web sitesi arasında gönderilip alınan bilgilerinin aslında bir ara web sitesi üzerinden geçtiğinden habersizdir. Bir suçlu, herhangi bir özel bilgiyi görmek ve işlemlerde değişiklik yapmak için ara web sitesini kullanabilir.

Tek Kullanımlık Parola: Tek oturum açma işleminde kullanılmak üzere oluşturulan bir paroladır. Zaman zaman, güvenli bir kanal aracılığıyla istemci ile sunucu arasında gönderilir ve alınır.
Açık Wi-Fi: Potansiyel olarak, bağlı olan kullanıcıların aygıtlarını ve etkinliğini (trafik) ağdaki diğer tüm kullanıcılara açık hale getiren, kısıtlamaların az olduğu ya da hiç bulunmadığı, halka açık bir ağdır.
Yama: Bir "düzeltme" olarak yayınlanan yeni bir yazılım parçasıdır. Çoğu yazılımın oluşturulması binlerce satırlık programlama dili gerektirir, bu nedenle bir geliştiricinin tüm güvenlik açıklarının kapatıldığından emin olması zordur. Giriş noktaları bilgisayar korsanları veya bir geliştirici tarafından keşfedildiğinde, yazılım satıcı firmaları genellikle düzeltme olarak yeni yazılım parçaları yayınlar.
Kimlik Avı Dolandırıcılığı (Saldırısı): Bilgisayar korsanları tarafından parolalar, banka hesapları veya kredi kartları dahil olmak üzere hassas bilgilerin ele geçirilmesi için kullanılan bir yöntemdir. Genellikle, kullanıcıya beklenmedik bir zamanda yasal bir kaynaktan gönderilmiş gibi görünen bir e-posta gönderilir. Bir bilgisayar korsanı, pek çok durumda, alıcıyı banka bilgileri gibi ele geçirmeye çalıştığı bilgilerle yanıt vermesi ya da kötü amaçlı bir bağlantıyı tıklaması veya bir eki çalıştırması için kandırmaya çalışır.
Fidye Yazılımı: Bir bilgisayardaki dosyalara erişimi kasıtlı olarak engelleyen bir tür kötü amaçlı yazılımdır. Bir bilgisayara bu amaçla tasarlanmış bir kötü amaçlı yazılım bulaşırsa, yazılım tipik olarak dosyaları şifreler ve şifrelerinin çözülmesi için bir "fidye" ödenmesini talep eder.
Belirteç: Bir ağ hizmetine erişim için yetki veren bir öğedir. Genel olarak, bir donanım güvenliği belirteci ya da kimlik doğrulaması belirteci, kullanıcıların bir ağ hizmetine erişime yetki vermesi için yanında taşıdığı akıllı kartlar ve anahtarlıklar gibi küçük donanım aygıtlarını ifade eder.
Truva Atı: Genellikle bir bilgisayar korsanının bir bilgisayara uzaktan erişim elde etmesine olanak sağlayan bir kötü amaçlı yazılım parçasıdır. Truva Atı bulaşmış olan bir sistem, bir suçlunun dosyaları karşıdan yüklemesi ya da kullanıcının tuş vuruşlarını izlemesi için bir giriş noktası yaratır.

İki Faktörlü Kimlik Doğrulaması: Bir kullanıcının iddia ettiği kimliğinin doğrulanması için iki farklı bileşenin kullanılmasıdır.
Virüs: Kişisel bilgisayarlara yönelik bir tür kötü amaçlı yazılımdır. Virüsler, ilk olarak disketlerin kullanımıyla birlikte ortaya çıkmıştır. Virüsler, tipik olarak bir bilgisayardaki bilgileri bozmayı, silmeyi veya değiştirmeyi ve ardından diğer bilgisayarlara yayılmayı amaçlar ve bazıları aynı zamanda fiziksel hasara neden olabilir.
Sanal Özel Ağ (VPN): Bir kullanıcının İnternet'i kullanırken anonim olarak kalmasına imkan tanıyan bir araçtır. Bir VPN, lokasyonu gizleyerek ve kullanıcının bilgisayarı ile ziyaret ettiği web sitesi arasında aktarıldığı sırada trafiği şifreleyerek anonimlik sağlar.
Su Kaynağı (Saldırısı): Belirli bir hedef kitlenin sıklıkla ziyaret ettiği bir web sitesine kötü amaçlı kod yerleştirerek belirli bir ilgi alanına sahip olan bir grubu hedefleyen bir saldırıdır. Örnek: 2013 yılında, bazı enerji ve altyapı hizmetleri şirketlerinin web sitelerini ziyaret edenler, bilgisayarlarına bulaşabilen kötü amaçlı bir koda maruz kalmıştır.
Beyaz Şapkalı Bilgisayar Korsanı: Bilgisayar korsanlığı yeteneklerini etik bir amaçla kullanan bir kişidir. Buna karşı, "siyah şapkalı" bilgisayar korsanı ise tipik olarak kötü amaçlıdır. İşletmeler, siber güvenlik yeteneklerini test etmek için genellikle beyaz şapkalı bilgisayar korsanları işe alır.
Solucan: Diğer bağlı bilgisayarlara bulaşmak için kendini çoğaltabilen bir kötü amaçlı yazılım parçasıdır. Kötü amaçlı yazılımlar, istismar etmek ve yayılmak için bir ağdaki zayıf sistemleri aktif olarak avlar.
Sıfır Gün (Saldırısı): Belirli bir tür yazılım istismarıdır, genellikle kötü amaçlı yazılımdır. Sıfır gün istismarını özgün kılan özellik, halk ya da yazılım satıcı firması tarafından bilinmemesidir. Bir başka deyişle, güvenlik açığından haberdar olan az sayıda insan olduğundan, kendilerini bunun kullanımından korumak için ″sıfır günleri″ bulunur.

Sosyal mühendislik saldırıları

Sosyal mühendislik saldırıları, parola veritabanları çalınarak yasal kullanıcı parolalarının elde edilmesi amacıyla kullanılabilir. Sosyal mühendislik saldırısı yöntemleri arasında kimlik avı dolandırıcılığı, su kaynağı saldırıları (watering holes) ve Truva atları yer alır.

Sistem ihlalleri ve kötü amaçlı yazılım bulaşmaları

Programlama kodundaki "hatalar", saldırganların bir sistemi ihlal etmesi ve "ele geçirmesi" için fırsatlar sunar. Varsayılan parolalar ve açık dosya paylaşımları gibi yapılandırma hataları da önemli güvenlik sorunları yaratır. Ağ tasarımı ve protokol zayıflıkları, kötü amaçlı yazılım bulaşmaları ve ilk "kenetlenme" saldırıları için giriş noktaları yaratabilir.

Ortadaki Adam (MitM) saldırıları

Ortadaki Adam (MitM) saldırıları, ağ trafiğinin arasına girilmesi, trafiğin yakalanması ve ardından serbest bırakılması için kullanılır. MitM saldırılarına yasal web sitelerinin kandırılması için İnternet alan adlarının veya mobil uygulamaların kullanılmasını ya da hassas verilerin yakalanması veya bunların "kopyalanması" için satış noktası (POS) kopyalayıcılar gibi fiziksel aygıtların kullanılmasını kapsayabilir.

MitM saldırıları, kimlik avı dolandırıcılığı (phishing) ve site trafiğini yönlendirme (pharming) saldırılarının gelişmiş bir türevidir. Bir suçlu, bu saldırılarda, gizli bilgileri görüntülemek ya da işlemleri değiştirmek için bir ara web sitesi kullanır. Böylece, kullanıcılar bir web sitesinde oturum açtığında ve çalışmaya başladığında, kendileri ile web sitesi arasında gönderilip alınan tüm bilgilerin bir suçlu tarafından ele geçirildiğini fark etmez.

İnternet protokolü (IP) sahtekârlığı

İnternet protokolü (IP) sahtekârlığı, erişimi bilinen IP ve ortam erişim denetimi (MAC) adresleri ile sınırlayan güvenlik sistemlerinin atlanmasını kapsar. Bu yöntemle, bir saldırgan, sistemlere erişmek için yasal bir uç noktasını taklit eder.

Sistem erişimi kimlik bilgilerinin çalınması ve istismar edilmesi

Yetkisiz bir kullanıcı, yasal sistem yöneticisi kimlik bilgilerini çalarak, bir veya daha fazla sisteme erişim elde edebilir. Bu senaryoda, bir saldırgan, A Sistemi için sistem yöneticisi kimlik bilgilerini çalar ve bunları Sistem B'ye erişmek için "akışın aşağısında" kullanır. Sonuçta saldırgan, iki sistem arasındaki "güven ilişkisini" istismar edebilir.

Hizmetin Engellenmesi (DoS) saldırıları

Bir saldırgan, anasistemin yasal kullanıcılara hizmet sunmasını önlemek için çok yüksek miktarda ağ trafiğini bir ağ anasistemine yönlendirebilir. Saldırganlar anasistemlerde başarıyla aşırı yüklenme yarattığında, potansiyel olarak sistem erişimini kısıtlayabilir ve diğer kullanıcılara hizmet sağlanmasını engeller. Buna Hizmetin Engellenmesi (DoS) veya Dağıtılmış Hizmetin Engellenmesi (DDoS) adı verilir.

Gelişmiş Sürekli Tehditler (APT'ler)

Gelişmiş Sürekli Tehditler (APT'ler), iyi finanse edilen, yüksek beceri düzeyine sahip örgütler veya ülke devletleri tarafından yaratılır ve genellikle belirli organizasyonları hedef alır. APT'ler, görünmez ve sürekli bilgisayar korsanlığı süreçleridir. APT'ler, aylarca atıl durumda kalabilir, ancak etkinleştiklerinde tipik olarak son teknoloji ürünü istismar yöntemlerini kullanırlar.