ZARARLI YAZILIMLAR

TEMEL BİLGİ TEKNOLOJİLERİ

DÜZCE ÜNİVERSİTESİ UZAKTAN EĞİTİM

VİRÜSLER

- Bilgisayar ortamına kullanıcının istemi, onayı dışında aktarılmış (trojans, worms) mevcut kullanıcı dosyalarını, bilgisayardaki yazılım ve/veya işletim sisteminin bütünlüğünü, erişilebilirliğini, gizliliğini tehdit eden yetkisiz kod parçaları ve küçük yazılımlar genel olarak virüs olarak adlandırılırlar. Bilgisayar virüsleri, bir bilgisayardan bir diğerine yayılmak ve bilgisayar sisteminin çalışmasına müdahale etmek amacıyla tasarlanmış program kodlarıdır.

VİRÜSLER

- Bilinen ilk bilgisayar virüsü, 1971 yılında BBN Technologies'de mühendis olan Robert Thomas tarafından geliştirilmiştir. "Creeper" virüsü olarak bilinen Thomas'ın deneysel programı, ARPANET'te ana bilgisayarları etkileyerek ve "I'm the creeper: Catch me if you can." teletype mesajını görüntüleyerek işlevini gerçekleştirdi.

BİLGİSAYAR VİRÜSÜ ÇEŞİTLERİ

PHISHING (OLTALAMA):

- Phishing, dolandırıcıların rastgele kullanıcı hesaplarına güvenilir kaynakların veya kullandığınız hizmetlerin taklit adresleri ve kopya içerikleri ile e-mail gönderdikleri bir çevrimiçi saldırı türüdür. Güvenilir bir firma veya kişinin kimliğine bürünüldüğü bir tür sosyal mühendislik saldırısıdır. Password (Şifre) ve Fishing (balık avı) kelimelerinin birleşimi ile ortaya konan bu saldırı atağında amaç Username ve Password bilgisi başta olmak üzere Bitcoin Cüzdanı, Kredi Kartı bilgilerinden tutun tüm abonelik verileriniz, program/oyun keyleriniz dahil çok kapsamlı şekilde bilgi elde etmeye yönelik olabilir.

RANSOMWARE (FIDYE YAZILIMI):

- Truva atı virüsü sınıfından olan ransomware türü, bulaştığı bilgisayarda yaptığı değişikliklerin geri alınması için herkes tarafından takip edilemediği bilinen ödeme sistemleri ile kazanç talebinde bulunur. En sık rastlanan bulaşma şekli ya kimlik hırsızlığı e-postalarının açılması yada kötü amaçlı program içeren bir web sitesinin ziyaret edilmesi sonucudur.

WORMS (SOLUCAN):

- Bilgisayarınızda bulunan ağ bağlantısı sayesinde herhangi bir yerleşik dosyaya gizlenmek zorunda kalmayan solucan, her bilgisayara ağ bağlantısı üzerinden bulaşabilir. En büyük farkı, kopyalanıp çoğalması için herhangi bir insan eylemine ihtiyaç duymamasıdır. Ağların yaygın olarak kullanılmasından önce, bilgisayar solucanları bir sisteme monte edildiklerinde, kurban sistemine bağlı olan diğer depolama aygıtlarına bulaşarak, depolama ortamları üzerinden yayılmıştır. USB sürücüler hala bilgisayar solucanları için ortak bir vektördür.

TROJAN HORSES (TRUVA ATI):

- Bir program ile bilgisayarınıza yüklenen bu virüs arka planda gizli olarak çalışır. Mesela en sinsi Truva Atı türlerinden biri, bilgisayarınızı virüslerden kurtardığını iddia eden ancak bunun yerine bilgisayarınıza Truva Atı bulaştıran bir programdır. Genellikle, Truva atı, masum görünümlü bir e-posta ekinde veya ücretsiz indirmede gizlenir. Kullanıcı e-posta ekini tıkladığında veya ücretsiz programı indirdiğinde, içine gizlenmiş olan kötü amaçlı yazılım kullanıcının bilgisayar aygıtına aktarılır, içeri girdikten sonra, kötü niyetli kod , saldırganın gerçekleştirmesi için tasarladığı görevi ne olursa olsun yürütebilir.

POLYMORPHIC (ÇOKLU FORM):

- Her bulaşmada kendini değiştirmektedir. Virüs programları bu virüsü önleyebilmek için tahmin yürütme yoluna dayalı teknolojiler kullanıyorlar, en tehlikeli virüs türlerindendir. Polimorfik virüs, yeteneklerini değiştirebilen veya temel işlevlerini veya özelliklerini değiştirmeden, temel kodunu değiştirme yeteneğine sahip kötü amaçlı yazılım türüdür.

BOOT SEKTÖR VIRÜSÜ:

- Boot sektör virüsü, hard disklerin boot sektörüne yerleşir. Ayrıca yapısı itibariyle bilgisayar hafızasına da yerleşebilir. Bilgisayar açılır açılmaz boot sektöründeki virüs hafızaya yerleşir. Bu tarz virüsleri temizlemesi oldukça zordur.

MULTIPARTITE (BÖLÜMLÜ VIRÜS):

- Boot ve dosya / program virüslerinin melezi olarak tanımlanabilir. Program dosyalarına bulaşır ve program açıldığında boot kayıtlarına yerleşir. Bilgisayarın bir dahaki açılışında hafızaya yerleşir ve oradan diskteki diğer programlara da yayılır.

BACKDOOR (ARKA KAPI):

- Backdoor, bir sisteme dışarıdan sızılabilmesi için o sistemde açık oluşturma işlemidir. Genellikle bazı portları açarak kendi üreticisinin ve/veya başka bir yazılımın sisteme sızmasını sağlayan yazılımlardır.

TRAP DOORS (TUZAK KAPISI):

- Tuzak kapısı, yazılım alanındaki Backdoor için yeni bir genişletilmiş jargondur. Tuzak kapısı, bundan haberdar olan biri için, normal güvenlik erişim prosedürlerinden geçmeden sisteme erişim sağlamasına izin veren bir programa gizli bir giriş noktasıdır. Tuzak kapısı bir sistemin yazılımını yapan kişi tarafından, yazılımın içine gizli bir şekilde yerleştirilen bir tuzak iletişim yazılımı veya donanımsal iletişim açığıdır. Bu programın çalıştığı bilgisayara veya bu donanımın bulunduğu bilgisayara virüsü yerleştiren veya bundan haberdar olan kişinin, uzaktan erişim yöntemiyle sistem korumasını aşarak sızması mümkündür.

EXPLOIT (SÖMÜRME):

- İşletim Sistemleri ve bazı programların açıklarını bulup bu açıkları kötüye kullanma yöntemi "exploit" diye adlandırılıyor. Exploit'ler ile sistem şifreleri görülebilir, sistemler hakkında bilgiler elde edilebilinir. Exploitler sistemin olağan olarak çalışmasına engel olurlar ve sisteme dışardan kod göndererek sistemi normal olarak çalıştığına ikna ederler ve genelde de yetkisiz erişim için kullanılırlar.

LOGIC BOMB (MANTIK BOMBASI):

- Mantık Bombaları, herhangi bir programın içerisine yerleştirilen virüs programlarıdır. Bazı şartların sağlanması durumunda patlayarak yani çalışmaya başlayarak sisteme zarar verirler. Bombalar, tüm dosyaları ve bilgileri silebilir veya işletim sistemini "göçertebilir".

SPYWARE (CASUS):

- İnternette dolaşırken, ziyaret edilen siteleri, bu sitelerin içeriklerini sık kullanılan programları internet üzerinden üreticisine gönderir. internette dolaşırken tuzak pencerelere tıklandığında bilgisayara kurulur.

ADWARE (REKLAM):

- Sadece kullanıcı ile ilgili bilgileri kullanmazlar aynı zamanda browser ayarlarını değiştirirler. Eğer anlam veremediğiniz reklamlar karşınıza çıkıyorsa ve browserınızın ana sayfası sizin istemediğiniz bir sayfa olarak ayarlanmışsa adware virüsü bulaşmış demektir.

MACRO (MAKRO):

- Bilgisayar uygulamaları ve bilgisayar programları ile dosyalara bulaşan makrolara sahip virüslerdir. Bu virüsler özellikle Microsoft Word, Excel gibi ofis programları uygulamalarında makro dili komutlarını hedeflerler. Word'de makrolar, belgelere gömülü komutlar veya tuş vuruşları için kaydedilmiş dizilerdir. Makro virüsleri, zararlı kodlarını bir Word dosyasındaki yasal makro dizilerine ekleyebilir. Makro virüslerinin son yıllarda yeniden dirildiğini gördüğü için, Microsoft, Office uygulamalarına 2016'da, güvenlik yöneticilerinin yalnızca güvenilir iş akışları için makro kullanımını seçebilmesinin yanı sıra bir kuruluştaki makroların tamamen engellemesine olanak sağlayan yeni özellikler ekledi.

KEYLOGGER (TUŞ-KAYIT):

- Keylogger, uzak bilgisayara kendi kurulumunu gerçekleştirdikten sonra genellikle kendini hiç belli etmeden çalışmaya başlar ve kaydettiği verileri programlandığı zaman aralıklarında hacker 'a iletir. Genellikle tüm klavye hareketlerini ara hafızasına alır ve transfer eder. Keylogger basitçe sizin klavyeden yaptığınız her vuruşu kaydeden ve bu kayıtları kişisel bilgilerinizi çalmak isteyen kişilere gönderen programlardır. Bu yolla sizin e-mail şifreniz, kredi kartı numaranız gibi hayati önem taşıyan bilgileriniz çalınabilir.

SCREENLOGGER (EKRAN-KAYIT):

- Keylogger ile aynı temel mantığa dayanır. Fare ile ekranda bir noktaya tıklamanız ile beraber aynı anda screen logger, adeta ekranın tamamının ya da küçük bir bölümünün (genellikle fare merkezli olarak küçük bir dörtgenin) o anki resmini çekerek bunları internet ortamında sabit bir adrese iletir.

SPAM (YIĞIN MESAJ):

- Spam, e-posta, telefon, faks gibi elektronik ortamlarda çok sayıda alıcıya aynı anda gönderilen gereksiz veya uygunsuz iletiler. En yaygın spam türleri reklamlar ve ilanlardır. Elektronik posta (e-posta), internet'in en eski ve halen en vazgeçilmez iletişim araçlarından birisidir. E-posta, fiziksel, alışıla gelmiş posta alımı ya da gönderiminin elektronik olanıdır ve internet üzerinden gerçekleştirilen, düşük maliyetli ve hızlı iletilen bir yapı olduğundan; güvenlik, kimlik denetimi gibi gereklilikler göz önünde bulundurulmamıştır ve bu yüzden e-posta altyapısı günümüzde internet'in en büyük problemlerine sebep teşkil etmektedir. Yığın ileti sadece e-posta ile sınırlı değildir. Diğer şekillerde de kullanıcının karşısına çıkabilmektedir; Hızlı mesajlaşma servislerinde, haber gruplarında, Web arama motorlarında, Web günlüklerinde (bloglarda), Cep telefonlarında

DIALER (TELEFON ÇEVIRICI):

- Çevirmeli telefon bağlantısı yapıldığında, sisteme sızıp sizin izniniz olmadan yurtdışı bağlantılı ücretli telefon araması yaparak, telefon faturanız üzerinden para kazanma yöntemidir. Dialere kapılan kullanıcı beklemediği bir telefon faturası ile karşılaşabilir. Bedava mp3, bedava program, crack linklerinin tıklanması, burayı tıkla veya tamam düğmeleri ile sitedeki java programı çalıştırılarak sisteminizi tuzağın içine çeker. Her ne kadar kapatmaya çalışsanız da tekrar tekrar açılmaya davet eder.

BROWSER HIJACKER (TARAYICI GASP):

- Browser Hijacker, bazı web siteleri tarafından, sayfalarının ziyaret sayısını arttırmak, kendi web sitelerindeki reklamların yüksek görüntülenme rakamlarına ulaşmasını sağlamak amacıyla web tarayıcınıza yerleştirilen, başlangıç sayfalarını ve arama sayfalarını değiştirebilen küçük bir program ya da registry ayarıdır. Eğer internet arama sayfalarınız ya da ana sayfanız sizin istemediğiniz bir şekilde değişiyorsa muhtemelen bilgisayarınızda böyle bir gaspçı program yer edinmiştir.

TRACKING COOKIE:

- Cookie yani çerezler internette gezdiğiniz siteler vb. ile ilgili veri barındıran basit metin dosyalarıdır ve bilgisayarınızda çerez (cookies) klasöründe bulunurlar. Pek çok site de ziyaretçileri hakkında bilgi almak için çerezleri kullanırlar. Örneğin bir sitede ankette oy kullandığınız ve her kullanıcının bir oy kullanma hakkı var. Bu web sitesi çerez bilgilerinizi kontrol ederek sizin ikinci defa oy kullanmanıza engel olabilir. Ancak çerezleri kötü niyetli kişiler de kullanabilir. Tracking cookie adı verilen bu çerez türü bulaştığı bilgisayarda internette yapılan tüm işlemlerin, gezilen sayfaların kaydını tutar. Hackerlar bu şekilde kredi kartı ve banka hesap bilgilerine ulaşabilirler.

DENIAL OF SERVICE ATTACK (HIZMET ENGELLEME SALDIRISI):

- Truva atlarının dayandığı temel düşünce kurbanın bilgisayarındaki internet trafiğini bir web sitesine ulaşmasını veya dosya indirmesini engelleyecek şekilde arttırmaktır. Hizmeti engelleme saldırısı truva atlarının bir başka versiyonu mail-bombası truva atlarıdır ki ana amaçları mümkün olabildiğince çok makineye bulaşmak ve belirli eposta adreslerine aynı anda filtrelenmeleri münkün olmayan çeşitli nesneler ve içerikler ile saldırmaktır. Benzer şekilde tüm TCP/IP servislerine veya her türlü iletişim protokolüne bu saldırıları özellikle zombi botnet ağları ile yapmak pek bilinen ve önlemi alınamayan bir atak türüdür,

KAYNAK

http://www.bilgisayarsistemleri.net/