Bilişim Suçlarının Çeşitleri ve Kullanılan Yöntemler

Çalışmanın Sahibi: Polatkan Akdağ

Sosyolojik bir konu olarak suç, insan doğasıyla ve çevresel faktörle açıklanmaktadır. Çevresel faktörler neleri ihtiva eder diye düşündüğümüzde ise hemen yaşadığımız doğa ile bir bağlantı kurmaya çalışırız. Günümüzde, normal bir doğal çevreye ilave sanal bir çevre kültürü yeşermektedir. Pek çoklarının sanal âlem ya da siber âlem dediği bu olgu artık bizi ne kadar etkiliyor? Bilgisayar başından her türlü işlemini gerçekleştiren ve ağlar arasında kaybolmuş bir birey çevresine ne kadar dikkat edebilir ya da insanlarla olan iletişimini ne düzeyde devam ettirebilir? Bu soruların cevapları elbette sosyologlar ya da psikologlar tarafından araştırılmaktadır, bu bağlamda yapılan araştırmalardan elde edilen verilere göre bireyler toplumdan kendini yavaş yavaş yalıtmaktadır, bunun bir sonucu ise kişide ruhsal bozuklukların oluşması ve depresyon halidir. Arkadaş veya aile ilişkilerinden uzaklaşan sosyal bir varlık olarak insan pek çok yönden sosyopat bir kişilik alt benliği yaratmaktadır. Konuya kriminolojik açıdan yaklaştığımızda ise bilişim suçlarını işleyen

bireylerin ki bu suçlar bireysel olarak işlenebileceği gibi toplu olarak da işlenebilir, genel itibariyle bir meslek sahibi genç ve zeki insanlardan olduklarını görmekteyiz. Günümüzde işlenen bilişim suçu mağdurlarının kim ya da ne olduklarına baktığımızda, karşımıza en çok ticari şirketler, kamu kurum ve kuruluşları ile banka ve telekomünikasyon kurumları çıkmaktadır . Bilişim suçunu işleyen bireylerin daha önce adi suçlardan dolayı kayıtlarının olmadığını ve suç mağdurlarının profilinden de anlaşılacağı üzere kendilerini zamane Robin Hood olarak gördüklerini söyleyebiliriz. Medya organlarının da bu tür suçluları zenginden alıp fakire veren kişi/kişiler veya halk kahramanı olarak tanımladığını belirtmek gerekir, bunun ötesinde internet üzerinde kendilerini hackerlerin bir araya geldiği ortam olarak tanıtan, binlerce üyesi olan forum, haberleşme ve paylaşım sitelerinde "Basında Biz" bölümü vazgeçilmezlerdendir. Tarihin her sayfasında bilgi hep bir güç olarak kullanılmış ve güçlüler ile bilgiye sahip olanlar ise hep zenginler olmuştur, fakat artık bilgiye ulaşmak için zengin olma gibi bir şart bulunmamaktadır, siber medeniyette her bilginin herkes tarafından paylaşılması inancı işte bu Robin Hood'ların arzusudur: bilginin serbest dolaşımı. Bilgisayar kaynaklı suç tiplerinde faillerde genel olarak, ya çalıştıkları iş yerinin kendilerine yetersiz gelmesi ya da işyerinden çıkarılma sebebiyle intikam ve ders verme duygusu, finansal zorluklar içinde bir yaşamı hak etmediği inancı, toplum içinde farklı bir birey olma ve bilgisayara karşı üstünlüğünü kanıtlama duyguları egemendir . Tüm bunlara rağmen bilişim suçlarında kriminal açıdan üzerinde durulan en büyük konu ise suçun kendisi olmaktadır. Suçun işleniş biçimi, işlenirken hangi bilgilerin kullanıldığı, teknik donanımın ne olduğu ve zamansal-tekrarlanabilir olup olmadığı konuları üzerinde durulmaktadır.

Bir devlet dairesini ya da bir özel sektör kurumunu düşündüğümüzde, bilgisayar olmasa acaba yapılacak işler günümüzde ne kadar zaman alır ve insanlar bu duruma ne kadar tahammül edebilirler. Bunun ötesinde sistemin çöktüğünü veya bir sorun gereği bir süreliğine işlemlere cevap vermediğini düşünelim. Bu durumdan etkilenmeyecek kurum ya da birey yoktur. Bilgilerimizi daha kolay ve her an ulaşabilecek şekilde sakladığımız dijital bellekler her şeyi depolama kabiliyetine sahiptir. Geçmişte de bir dosyalama sistemimiz vardı fakat hem maliyet yönünden zararlı hem de depolama ve ulaşılabilirlik yönünden fazla hantal ve zahmetliydi. Kısaca düşündüğümüzde, dijital veri tabanlarının ne kadar kullanışlı ve yararlı bir sistem olduğunu kavrayabiliriz. Fakat her dijital veri tabanı ya da bellek sistemi güvenilir midir? Bilgisayar ağlarına emanet ettiğimiz kişisel bilgilerimiz, gizli dosya ve klasörlerimiz artık sadece bizim ulaşabileceğimiz bir yerlerde mi? Yoksa bu bilgilere herkes ulaşabilir mi? Konuya güvenlik olarak yaklaştığımızda, neyin ne kadar güvenli olabileceği konusunda bile şüphelerimiz vardır. Hiç kimsenin ya da ilgili kişiler haricinde ki insanların bilmeleri gerekmeyen verilerimizi korumanın yollarını düşünürüz ama bu yöntemlerin ne kadar güncel ya da güvenli olduğunu bilemeyiz. Teknolojiye bağlı olarak son 20 yılda artan ve artmaya devam edecek olan bilişim suç ve suçlularının özelliklerine değinmek gerekirse; genel itibariyle bilişim suçları bilgisayar ve bir ağ üzerinden bilişim teknolojileri kullanarak gerçekleştirilir, yakalanma riski sıfıra yakındır, elde edilmesi amaçlanan çıkarım yüksek bir oranda elde edilir, bu tür suçların doğası gereği yeni bir suç türü olması kanun ve düzenlemeleri yetersiz ve eksik kılmaktadır, pek çok adi suç türüne göre maddi ve manevi hasar daha yoğundur, suç mağdurları genel olarak bilgisayar sistemleri konusunda az bir bilgiye sahip kullanıcılar ile

kamu ve finans sektörü kuruluşlarıdır, bahse konu kuruluşların güvenlik açıklarını kötü imaj endişesiyle kolluk kuvvetlerine bildirmemeleri söz konusudur, suça karışan bireylerin genelde 30 yaş altı kimseler olması, fail profilinin eğitimli ve bilinçli kişiler olması ayrıca kendilerine fazla güven duymaları olarak özetleyebiliriz.

Bilgisayar sistemlerine yönelik saldırılar üç ayrı alanda incelenmektedir ve fiziksel, sentaktik ve semantik olarak adlandırılmaktadır. Fiziksel saldırılarda, bomba gibi konvansiyonel silahlar kullanılır, sentaktik saldırılar, ağ ve bilgisayar sistemlerinin çökertilmesine yönelik virüs tipi yazılımları içermektedir. Semantik saldırılar ise daha zekice planlanmış bir yaklaşımı ifade etmektedir. Semantik saldırılarda saldırgan, sistemin hata üretmesini ve tahmin edilmeyen sonuçların ortaya çıkması amaçlar. Sentaktik saldırılar zararlı yazılımlar olarak bilinen malware ile gerçekleştirilir. Bu saldırılar, virüsleri, kurtçukları ve Trojan atlarını kapsar. En çok bilinen zararlı yazılım bulaştırma yöntemi e-mail içine gizlenip gönderme eylemidir. DDoS ve DoS saldırıları da sentaktik saldırılar kapsamına girmektedir. Bu tür saldırılarda en çok kullanılan yöntem ise ping atma işlemidir. Ping, verilen internet adresine ulaşabilirliği doğrulayan standart internet işlemidir. Yoğun şekilde yapılan ping ataklarında sistemde bir aşırı yüklenme meydana gelir, bu şekilde sistemin veya ağın internet veya intranet hizmeti alması engellenir. Semantik saldırılar ise yanlış bilginin neşredilmesi veya bilginin değiştirilmesini kapsar. E-mail, forum siteleri ve mesaj panelleri vasıtasıyla daha kolay bir şekilde yayılması sağlanan yanlış bilgilerle, insanlar, kamu ve özel sektör kurumları yönlendirilir . Bilişim sektörünün pek çok yararının yanında olası zararlarının da varlığı, üzerinde daha derinlemesine ve bilinçli araştırmaların yapılması gerekliliğini ortaya koymaktadır. Bilişim suçlarının kategorize edilmesinde pek çok yöntem kaleme alınmıştır. BM'nin 10 – 17 Nisan 2000 tarihleri arasında Viyana'da gerçekleştirdiği 10. kongresinde, Suçun Engellenmesi ve Suçluların Tedavisi konulu bir toplantı düzenlenmiş, bu toplantıda bilişim suçları beş ayrı sınıfa ayrılmıştır. Bu sınıflandırmaya göre;

a) İzinsiz girişler,
b) Elektronik veri ve yazılımları değiştirme ya da zarar verme,
c) Bilişim sistemini ya da network fonksiyonlarını sabote etme,
d) Bilişim sistemi ya da network üzerindeki verileri yetkisiz olarak durdurma veya farklı bir sisteme yönlendirme,
e) Bilgi casusluğu amacı ile yapılan her türden eylem, bilişim suçu olarak tasnif edilmiştir. Avrupa Konseyi Siber Suç Sözleşmesi, Interpol Bilgisayar Suçu El Kitabı ya da Birleşmiş Milletler Bilgisayar Suçunu Önleme El Kitabı tasnifleme konusunda bizlere örnek oluşturabilir. Fakat eserin esas konusundan uzaklaşmamak maksadıyla bilişim suçları bu eserde iki ana başlık üzerinden işlenecektir.

Çıkar Amaçlı Bilişim Suçları

Suçun sosyolojik tanımı içerisinde, bireylerin gerek farklı motivasyonlarla gerekse salt çıkar elde etmek maksadıyla işledikleri suçlar bir çıkar ve amaca hizmet eder. Yeni yeni gelişen bilişim teknolojilerinin ise kötü amaçlı kullanımı esas itibariyle bireylerin merak arayışından doğmuştur. Bireysel ya da kitle halinde işlenebilen bu suçlar genel kullanıma açık okul, kütüphane, internet kafe gibi mekânlarda ya da şirket bilgisayarlarından herhangi biriyle icra edilir. Çünkü bilgisayar kullanımını ileri derece tekniklerle gerçekleştiren bu art niyetli kimseler her bilgisayarın da arkasında bir iz bırakacağını bilir. Çok az tecrübe sahibi kişiler ya da aşırı motive bireyler genelde kendi bilgisayarlarını kullanır, bununda farklı sebepleri olabilir, örneğin tecrübesizlik ya da meydan okuma gibi.

Suçun oluşmasında pek çok motivasyon söz konusudur, kendini ispatlama, gruba dahil olma, para kazanma, zarar verme, intikam, merak ya da ırkçılık gibi daha da uzatılabilecek fakat siyasi olmayan suç motivasyonlarından bahsedebiliriz. Çıkar amaçlı bilişim suçlarında bireysel saldırıların yanı sıra organize suç şebekelerinin faaliyetlerini de görmekteyiz. Çocuk istismarı, cinsel amaçlı sömürü ya da organ kaçakçılığı gibi pek çok organize suç türü günümüz koşulları itibariyle kendini internet ortamında da göstermektedir. Çekirdek hücre sistemi içerisinde dışarıya bilgi sızdırmadan, maksimum hızda ve minimum zamanda elde etmeyi amaçladıkları hedefe ulaşabilen zamanımızın organize şebekeleri, ticari faaliyette bulunan kurum ve bankalara yönelmiş durumdadır. İstanbul'da vadeli hesaplara ait bilgileri, banka müşterilerinin bilgisayarlarına Trojan göndererek ele geçiren bir organize örgüt ya da Antalya'da çocuklara karşı cinsel saldırılar gerçekleştiren bir suçlunun, bahse konu çocukların fotoğraflarını internet üzerinden yayınlaması artık günümüz suç örneklerindendir . Çıkar amaçlı bilişim suçlarını;

1. ***Bilgisayar sistemlerine ya da bilgisayar ağlarına yetkisiz olarak erişmek,***
2. ***Bilgisayar veya ağ sistemlerinin yetkisiz olarak izlenmesi,***
3. ***Kendisine ait olmayan dijital hesabın kötüye kullanımı,***

4. ***Bilgisayar ya da iletişim sistemlerinin, bilgisayar verileri veya programlarına girilmesi, yüklenmesi, değiştirilmesi, silinmesi veya ele geçirilmesi suretiyle engellenmesi,***
5. ***Bilgisayar ve iletişim teknolojileri kullanarak verilerin alınması, girilmesi, değiştirilmesi, silinmesi yoluyla kendisine veya başkasına yasadışı ekonomik menfaat temin etme veya mağdura zarar verme,***
6. ***Bankamatik sistemlerinden yapılan dolandırıcılık ve hırsızlık,***
7. ***Bilgisayar yazılımların izinsiz olarak çoğaltılması, satışı, kopyalanması, dağıtımı ve kullanımı,***
8. ***Kanuna aykırı yayınların saklanmasında ve dağıtılmasında bilgisayar sistem ve ağlarının kullanılması,***

9. Farklı amaç ve niyetlerle ticari ve meslek sırlarının, bilgilerinin satılması, kullanımı, transferi, dağıtımı, ifşası ya da elde edilmesi,

10.Bir başkasının ya da bir kurumun bilgilerini kullanarak hile ile menfaat sağlama ya da zarar verme, şeklinde bir ayırıma gitmek suretiyle inceleyebiliriz.,

Çıkar Amaçlı Bilişim Suçlarında Kullanılan Yöntemler

Çöpe Dalma

Daha ziyade kullanılan bilgisayarın hafızasında kalan bilgilerin silinmiş olsa dahi EnCase tarzı adli bilişim olaylarında da kullanılan yazılımlar vasıtası ile geri getirilmesi, geri getirilen bilgiler ile arzu edilen bilgilerin ayıklanması ve kullanılabilir olanların ele geçirilmesi olarak tanımlanabilir. Çöpe dalma ayrıca, bilgisayar çıktılarından arta kalan parçaların bir araya getirilmesi vasıtası ile bilgi etme amacıyla da icra edilebilir. Kurumsal çalışma ortamlarında, içeriden veya dışarıdan tehditler tarafından bu tür bilgilerin elde edilmesi olasıdır. ATM cihazlarının yanında bulunan çöp tenekelerinde işlem sonu hareketleri gösterir fişlerin üzerinden elde edilebilecek bilgiler ve atık kâğıt toplama kutularına gelişi güzel atılan önemli veya gizli içerikli evraklardan bu tür bilgiler, saldırı amacı taşıyan kişiler için önemli ipuçları barındırdıklarından toplanır. Bu tür bilgi toplama yönteminde zaman ve işe yarar bilgi azlığı, saldırganın nihai amacına ulaşmasını zafiyete uğratacağından, saldırı motivasyonu taşıyan suçlular için bu tarz eylemler çokça tercih edilen yöntemlerden değildir.

Gizli İzleme

Veri dağılımının yapıldığı alt yapılara dışarıdan yapılan fiziksel müdahalelerle dahil olunarak veri akışının izlenmesi şeklinde olabileceği gibi, bilgisayar ekranlarının yaymış olduğu elektromanyetik dalgaların yakalanarak, görsel olarak ekran görüntüsünün elde edilmesi şeklinde de icra edilmektedir. Veri işlem merkezlerine yerleştirilen vericilerle, uzak noktalardan nakledilen verilerin incelenmesi ve takip edilmesi de mümkündür. Gizli dinleme, organize suç örgütleri ve terör örgütlerinin ilgisini çektiği kadar devlete ait istihbarat kurumlarının da ilgisini çekmektedir. Organize örgütler ve terör örgütleri genel itibari ile telefon konuşmalarından uzak durmaya gayret göstermektedir. Adli yargılama

safhasında suç örgütünün deşifre edilmesi amacıyla alınan iletişimin dinlenmesi kararı, suçluların önüne tape edilmiş konuşmalar olarak konduğu için, suçtan dolayı içeri girmiş ve çıkmış şebeke elemanları veya suç unsuruna rastlanmamış telefon görüşmeleri sahibi kişiye yapılan tebligatlar nedeniyle, suçlular telefonla konuşmamaya, konuşmaları kendi aralarında şifrelemeye, bununda ötesinde gizli buluşma ve yüz yüze görüşme yapmaya başlamıştır. Kendini gelişimin kucağına bırakan organize suç ve terör örgütleri için ise durum farklıdır. Her ne kadar yukarıda bahsedilen önlemler bu gruplar tarafından devam ettirilse de, iletişimin hızlı ve coğrafik sınır tanımaksızın devam ettirilebilmesi için internet ağları kullanılmaya devam etmektedir. Bilgisayar temelli telefon görüşmeleri, mail adresleri kullanarak yapılan iletişim, chat odaları denilen çeşitli konuşma platformları, takibin zor fakat iletişimin global olarak sağlanabilmesine yarayan yeniliklerdir. Günümüzde insanlar telefon numaralarını veya mail adreslerini kolaylıkla değiştirebilmektedir. Özellikle paket anahtarlamalı ağ sistemi iletişim hizmeti sağlama ve merkezi olmayan iletişim imkânına olanak sağlamaktadır. Voice – over – Internet – Protokol dediğimiz VoIP, standart iletişimin önüne geçmiş yaygın bir iletişim hizmeti sunmaktadır. Sesli görüşmenin ötesinde görüntülü görüşme imkânı da sağlayan bu teknoloji suç ağları arasında kesintisiz iletişimin yeni trendi olmuştur .

Veri Hırsızlığı ve Dolandırıcılığı

Bilgisayarda bulunan verilerin içeriğini veya önceliğinin değiştirilmesini içeren veri dolandırıcılığında, bilginin değişime uğramasının sebebi bir virüs, veri tabanı veya uygulama yazılımı programcısı ya da bilginin olduğu ortama giren ve verileri manüel olarak değiştiren herhangi biride olabilir. Şüpheli, işlemin yaratılmasına, kaydedilmesine, deşifre edilmesine, kontrol edilmesine, aktarılmasına veya verinin yayımlanmasına dahil kişide olabilmektedir. Bilgisayar bağlantılı suçlar içinde neredeyse hiç bilgisayar bilgisi olmayan biri tarafından bile işlenebilecek bu suç türü oldukça basit bir yöntemdir. Suçun işlenmesinin kolaylığına karşın, failin veri dolandırıcılığıyla yaratabileceği maliyet oldukça büyük olabilmektedir. Banka hesabı veri giriş kısmına online ulaşabilen bir failin, kendi

hesabının sonuna ekleyeceği birkaç sıfırın maliyeti oldukça yüklü olacaktır. Bu tür suç tipiyle başa çıkabilmek için kurumların iç hizmet uygulamalarını kontrol edebilen politikalar geliştirerek, bu politikaların uygulanmasını sağlaması gerekmektedir. İç denetim mekanizmalarının sağlıklı çalışmaması, içeriden veya dışarıdan gelebilecek bu tür tehditlerle başa çıkamama sonucunu doğuracak, bu durumda kurumda güvensizliğe, işlerin aksamasına ve imaj zedelenmesine sebep olacaktır. Aldatma ayrıca, hedef alınan sistemin veya alt yapının istem dışı yanlış bilgi üretmesi ve üretilen yanlış bilginin doğruymuş gibi işlem görmesi olarak da kendini gösterebilir . Mersin Asayiş Şube Müdürlüğü Dolandırıcılık ve Yan Kesicilik Büro Amirliği tarafından 2008 yılında tamamlanan operasyonda, suç şebekesi içinde teknik bilgi sahibi bilgisayar uzmanlarının ve TEDAŞ görevlilerinin de olduğu bir grup suçüstü yakalanmıştır. Bu operasyonda dikkati çeken nokta davanın devam etmesinden kaynaklı burada ismi zikredilmeyecek olan büyük iş merkezlerinin elektrik sayaçlarını bu şebeke vasıtası ile sıfırlaması veya olması gerekenden daha aşağıya çektirmesidir. Dolandırıcılık bürosu tarafından ele geçirilen dizüstü bilgisayarda, şebeke elemanları tarafından oluşturulmuş bilgisayar yazılımı ile elektronik sayaçların sayısal veri ve değerlerinin değiştirildiği anlaşılmıştır. Sıradan vatandaşların da bu suç şebekesinin faaliyetlerinden faydalandığını belirtmekte yarar vardır. Şebeke yaptığı bu işlemler sayesinde yüklü miktarda para kazanmıştır ve bu hırsızlığın devlete olan maliyeti net olarak hesaplanabilmiş değildir.

Bukalemun

Çoklu ağ sistemlerinde kullanıcılara ait bilgileri gizli bir dosya içerisine kaydederek, kendini belli etmeden arka planda çalışan sistem yazılımıdır. Bilgisayar bağlantısının geçici bir süre mantıklı bir sebep yüzünden tekrar açılıp kapanacağı veya sistemin kapanması gerektiğini kullanıcıya ileterek bilgisayar bağlantısının kapanması sağlayan bu yazılım, kullanıcı tarafından bilgisayar yeniden işlem görürken gizli dosyalama yaptığı kullanıcılara ait bilgileri ilgili kişiye iletir. Böylece fail kişisel bilgi hırsızlığı yöntemi ile dolandırıcılıktan hırsızlığa her çeşit suç türünü işleyebilir.

Salam Tekniği

Banka hesaplarında, küsuratların bulunduğu son haneler fail tarafından oluşturulan başka bir hesaba aktarılır. Birden fazla hesap için yapılan bu uygulamayla, uzun vadede müşterilerin hesaplarından alınan ufak miktarlar muhatapların farkında olamayacakları bir sistematiğe göre biriktirilir. Daha çok içeriden tehdit olarak bilinen bu yöntemin önüne geçebilmek yine iç denetim mekanizmalarının oluşturulması ve politika haline getirilerek uygulanması gerekmektedir.

Zararlı Yazılımlar

Genel olarak bilgisayar – veri sabotajı, bilgi elde etme, reklam yayınlama ve saldırı başlatma amaçlarıyla dizayn edilen her türden kodları ifade eden zararlı yazılımlar içine, botnetleri, Truva atlarını, spamları, virüsleri, solucanları, rootkitleri, spywareleri, zaman – mantık bombalarını, arka kapıları (backdoors) ve saydığımız tüm bu zararlı yazılımlardan iki veya daha fazlasını aynı anda ihtiva eden combo malwareleri dâhil edebiliriz. Organize

suç şebekelerinin bu tür yazılımları kendi amaçları ve çıkarları için kullandıkları veya kullanamaya çalıştıklarını yaşanan pek çok örnekten ötürü biliyoruz. Bu gruplar içerisinde faaliyet gösteren bireyler, dünyanın herhangi bir yerinden eylemlerini yönetebilmektedir. Birlikte hareket ederek sistemleri hackleyen organize şebekesi üyeleri, sisteme aşırı yükleme yaparak sistemi yavaşlatmakta veya sistemin devre dışı kalmasını sağlayarak düzeltme için fidye istemekte, sisteme dahil olarak kredi kartı bilgilerini çalmakta, bu bilgileri yine online pazarlarda açık arttırma sistemine göre pazarlamakta ve satmaktadır. Ayrıca siber suçlular elde ettikleri mail adres bilgilerini kullanarak bağlantı listesinde olan tüm kişilere spam şeklinde mailler atarak dolandırıcılık yapmaktadırlar . Love Letter solucanı ile İsveç Union Bank ve Amerika'da faaliyet gösteren en az iki bankanın hesap şifrelerine erişim sağlayan kimliği belirsiz kişilerin organize bir faaliyet gösterdikleri olayda organize örgütlerle teknik uzmanlar arasında bir ilişkinin yaşandığı inancı kuvvetlenmektedir . Bilginin en büyük güç olduğu günümüzde, yazılımlar içine yerleştirilen ve kullanıcı tarafından fark edilemeyen arka kapılar ile sistemlere girilmekte, sisteme, kuruma, çalışanlara ve çalışanların tüm kişisel bilgilerine ait veriler elde edilmekte, isteğe göre çıkar amaçlı olarak her türlü suçta kullanılmaktadır.

Veri sistemleri üzerinden büyük şirketlerin alt yapılarına sızan ve sistemleri tamamen veya kısmen işleyemez hale getirip tehdit eden organize örgütler, tehdidin ortadan kalkması için yüklü miktarda paralar talep etmekte, sonuçta istedikleri geliri elde edip yeni yöntemlerini geliştirmeye devam etmektedirler. Anlık işlem hacmiyle milyar dolarlar kazanan firmaların alt yapılarının işleyemez hale gelmemesi için ödemek zorunda kaldıkları bu türden haraçlar genel olarak gizli olarak kalmakta ve rapor edilmemektedir. FBI, Amerika'da meydana gelen bilgisayar suçlarının hemen hemen her türünün endüstri sektörünü etkilediğini ve yıllık maliyetin 400 milyar dolar olduğunu tahmin etmektedir. İngiliz Sanayi ve Ticaret yetkilileri ise bilgisayar suçlarının 2005'ten 2006'ya % 50'lik bir artış gösterdiğini ifade etmektedir. Güvenlik ihlalinin sebep olduğu maliyete örnek olarak TJX şirketinin yapmış olduğu harcamalar verilebilir. TJ Maxx şirketinin uzantısı olan TJX şirketi 2006'dan bu yana çalınan 45 milyondan fazla kredi kartı ve bu kartlara ait numaralar için 2008'in ilk çeyreğinde on iki milyon dolarlık bir bütçe ayırmıştır. Bu para, araştırma, devam eden güvenlik ihlalleri, bilgisayar güvenliğinin geliştirilmesi, müşterilerle kurulan iletişim ve diğer masraflar için kullanılmaktadır. TJX şirketi gelecekte karşılaşacakları davaların yol açacağı zararlarla, kaybedilen her dava için 100 dolarlık bir ödeme yapılacağını varsayarak, toplamda 4,5 milyar dolarlık bir zararla karşı karşıya kalacaklarını tahmin etmektedir .

Phishing Yöntemi

Phishing olarak bilinen yöntem esasında İngilizce fishing yani balık tutma fiilinden üretilme bir tabirdir. Hedefin atılan yeme düşmesi beklenir ve ardından gerekli bilgiler elde edilerek dolandırıcılık fiili işlenir. Esasında hacking dünyasında fake mail olarak da ifade edilen yöntemle hedef kişi kandırılır. Örneğin, Hotmail servisinin ara yüzünde mail adresinin ve şifrenin yazıldığı sayfa görüntüsü, hedef kişinin veya herhangi birinin anlayamayacağı derecede profesyonellikte bilgisayar diliyle yeniden yazılır. Yazım sırasında girilen kodlar, hedef kişi kendi şifre ve mail adres bilgilerini sahte yazılıma yazdığında sahte yazılımı yazan kişiye ait mail adresine hedef kişinin bilgileri mail yoluyla gönderilir veya failin uygun göreceği bir adrese bu bilgiler gönderilir. Böylece fail elde etmek istediği bilgileri alır ve kendi konusu ile ilgili faaliyetlerine devam eder .

Bununla birlikte hedefin işlem yaptığı finans veya herhangi bir kurumun hazırlanmış fake ara yüzü, hedefe mail yoluyla gönderilir ve eksik ya da yanlış bilgilerin olduğu ve düzeltilmesi gerektiği ifade edilerek kişisel bilgilerin yeniden girilmesi istenir. Hedef kişi gönderilen maildeki linke tıkladığında sanki gerçekten her zaman muhatap olduğu site görüntüsüyle karşılaşır fakat gerçek farklıdır. Oltaya gelen hedef bilgileri girer girmez yazılım içindeki kodlar doldurulan hanelerin tamamlanmasıyla bilgileri faile mail yoluyla gönderir. Son olarak bilinen site adreslerinin benzerleri vasıtası ile dolandırıcılık fiili icra edilebilir. Ulusal veya uluslar arası bir bankanın online hizmet veren internet adresinde yapılan ufak bir harf değişikliği, arama motorunda yanlış adres bilgisini yazan kişiye pahalıya mal olabilir. Son zamanlarda gerek arama motorları gerekse kurumlar bu tür dolandırıcılık olaylarının önüne geçebilmek için denetim mekanizmalarını ciddi tutmaktadırlar. Yinede bu tür dolandırıcılık olaylarının yaşandığını söyleyebiliriz. Arama motorunda “yahoo” yazmak yerine yanlışlıkla “yehoo” yazdığınızda spamlarla veya zararlı kodlarla dolu bir siteye yönlendirilebilirsiniz. Sahte yazılımların yanında birde sahte vaatlerle oltaya getirme yöntemi vardır. 419 dolandırıcılı olarak da adlandırılan bu yöntem genel olarak Nijerya kökenlidir. 419 tabiri Nijerya’da işlenen bu suçun karşılığı

uygulanan yasal yaptırımın kanun kodunu ifade etmektedir. 1990'lı yılların başlarından bu yana özelikle Amerika'yı hedef almış bu dolandırıcılık faaliyeti son zamanlarda tüm dünyaya yayılmış vaziyettedir. Sömürülmüş bir toplum olarak kendilerini gören Nijeryalıların intikam duygularından yola çıkarak kendi haklarını alma mantığı bu suçun çıkış noktasıdır. Hedefe gönderilen mailler aracılığı ile iş yapma imkanı olduğuna dair bildirimlerde bulunulur. Nijerya Merkez Bankası veya İçişleri Bakanlığı antetli dokümanlarla oyun sürdürülür. İletişim bilgileri hedefe iletilir, güven duygusunun yaratılması için telefonun başında bekleyen kişi büyük bir işyeri veya kamu kurumu imajı vererek telefonu cevaplar. Nijerya'da kullanamayacağı paranın birlikte kara dönüştürülmesi, bir koyup on alma imkânının varlığı gibi insanların para kazanma hırslarını kullanan dolandırıcılar, nihayetinde hedefin banka bilgilerini, kişisel bilgilerini ve iletişim bilgilerini göndermesi konusunda ikna ederler. İkna olanlardan alınan bilgilerle dolandırıcılığın birinci aşaması tamamlanır.

Hedef kişiye ait banka hesapları boşaltılır ve aradan bir müddet zaman geçmesi beklenir. Bu kez ikinci aşama devreye girer ve paranın akıbeti ile ilgili bilgiler sanki yine bir resmi kurum statüsü içinde hedefe gönderilir, hedefin parasını alabilmesi için ya ülkeye davet edilir veyahut diğer hesap bilgileri istenir. Hedef kaybettiğini alabilmek için ikinci kez hesap bilgisini gönderdiğinde yine dolandırılır. Daha kötüsü parasını alabilmek için ülkeye davet edilenlerin başına gelir. Hedef uçaktan iner inmez takibe alınır, taksici hedefi havalimanından alarak gerçek olmayan iş adresine doğru götürür. Taksici ücreti karşılığı fahiş miktarda para talep eder ve alır. Telefon numarasından yola çıkarak elde edilen adres bilgisi boş bir eve veya araziye çıkar, zaten hedefe verilen adres yanlıştır. Hedef sonuçta iki kere zarara uğratılarak dolandırılır veya ülkeye geldiğinde kaçırılarak ailesinden veya ülkesinden fidye talep edilir. Bu tür suç şebekelerinde her türden aktivite bulunmaktadır. Hedefin öldürülmesine kadar giden bir sürecin işlemesi içten bile değildir. Phishing yönteminde uygulanan bir diğer dolandırıcılık şekli ise hedef şahsın ev veya iş adresine gönderilen mektuplarla ya da mail adreslerine gönderilen iletilerle hedefin ikramiye kazandığına inandırılmasıdır. Yine para kazanma hırsına yenik düşen hedeflerin iletişime geçmesi beklenir. İletişim gerçekleştikten sonra hedef tarafından sözde kazanılan ikramiyenin teslimi için banka hesap bilgileri hedeften istenir. Alınan hesap bilgileri ile hedefe ait banka yatırımları dolandırıcı tarafından ele geçirilir, bunun yanında hesap bilgilerinin alınmasından sonra paranın havale edilebilmesi için bir havale ücreti de hedeften talep edilir. Nihayetinde oltaya gelen hedef, fail tarafından iki kez dolandırılır. Sonuç olarak dolandırıcılar kişilerin bilgisizliklerinden veya zaaflarından faydalanmaktadırlar. Fiziksel hayatta dikkat ettiğimiz şeylere sanal dünyada da dikkat etmemiz gerçeği burada bir kez daha karşımıza çıkıyor.

Key Logger ve Screen Logger

Daha ziyade kurum içi tehdit algılaması nezdinde değerlendirilmesi gereken klavye ve ekran üzerinde yapılan işlemleri kaydeden bu yasal olmayan davranış şekli ile hedef kişinin bilgisayar üzerinde yaptığı hesap açma faaliyetleri, girdiği sitelerde yazdığı profil ismi ve şifre numaraları faile bir mail aracılığı ile gönderilir veya fail, hedef bilgisayardan kalktıktan sonra onun yerine oturarak bilgileri alır ve amacına ulaşır. Ayrıca toplu

kullanım alanları olan internet kafelerde de, bu tehditle karşı karşıyayızdır. Fail elde etmek istediği bilgileri alabilmek için bu program ve yazılımları herhangi bir bilgisayara yerleştirir. Ardından kendisi başka bir bilgisayarda işlemlerini devam ettirirken, tuzak bilgisayara oturan hedefe ait tüm kayıtlar saklanmaya başlanır. Tutulan loglar daha önce bahsettiğimiz üzere ya faile mail yoluyla gönderilir yada fail hedef kişi bilgisayardan kalktıktan sonra onun oturduğu bilgisayara oturarak kayıtlı bilgileri alır ve amacına ulaşmış olur. Hedef bilgisayara gönderilen bir yazılımın içine saklanmış bu tür veri kaydedici programlarla da fail amacına ulaşabilir. Sizin farkına varmadan açacağınız bir resim, bir Microsoft Office programı da bu türden az yer kaplayan yazılımların saklanmasına olanak sağlayabilmektedir. Masumane olarak açtığınız sıradan programlarla arka planda sizin göremeyeceğiniz şekilde çalışmaya başlayan bu tür yazılımlar internet ortamında hacker platformu olarak kullanılan kimi forum sitesinde mevcuttur ve failler tarafından kullanılmaktadır.

TOR

Proxy yazılımıyla birlikte çalıştırılması önerilen TOR yazılımının temel çalışma prensibi kullanıcıya ait IP bilgisini takip edilmeyi minimum seviyeye çekerek, veri alış verişi esnasında kullanıcıya ait konum bilgilerinin gizlenmesidir. İnternet üzerinde web siteleri ve MSN, ICQ, IRC gibi iletişim kanalları da dâhil olmak üzere, TCP protokolü ile çalışan tüm uygulamalar için bir maskeleme sistemi oluşturan TOR yazılımında, bağlantı esnasında oluşan veri paketleri birbiri ardına eklenmiş TOR sunucuları üzerinden hareket eder ve iletişimin güvenli bir şekilde gerçekleşmesini sağlar. Onion Router olarak da adlandırılan bu iletişim modelinde, gönderilen istek TOR sunucularından geçerek rasgele bir rota takip eder. Sistemin kullanılmasında hedeflenen amaç, saldırganın hedefe ulaştığında görünen IP adresinin TOR tarafından oluşturulmuş sunucu adresi olarak gözükmesidir. TOR yazılımı veri güvenliğini sağlamak amacıyla ayrıca kendi içinde bir şifreleme tekniğini kullanır. Bu şifreleme ile kendi içinde bir kalkan oluşturan TOR yazılımı, sunucular arasında bir birini tanıma özelliğini ortadan kaldırarak, sunucuların kendinden bir önceki ve bir sonraki sunucuyu tanımasına olanak sağlamaktadır. Yani sunuculardan hiç biri gidilecek rotanın ne olacağını bilmemekte, saldırgan tarafından sunucular hücre sistemi ile yönetilmektedir. Yazılımın bir Proxy ile desteklenmesiyle, cookie bilgilerinin oluşturacağı güvenlik açığı da bertaraf edilmektedir. TOR yazılımına uygun birkaç Proxy yazılımından biri olan PRIVOXY adlı program, son dönemde saldırganlar tarafından en çok tercih edilen yazılımdır.

[status draft]
[nogallery]
[geotag on]
[publicize off|twitter|facebook]
[categoryistihbarat]
[tags SUÇ DOSYASI, Bilişim Suçları, Çeşit, Yöntem]