VoIP ve ÜCRET DOLANDIRICILIĞI

Ali KATKAR, Selin KAMAŞ, Berna ÜST

Netaş, Siber Güvenlik Birimi, İstanbul

akatkar@netas.com.tr, skamas@netas.com.tr, bernau@netas.com.tr

Özet

Haberleşme sektöründe az maliyet ve kurulum kolaylıkları nedenleriyle internet tabanlı teknolojilere yönelim söz konusudur. Internet üzerinden ses iletimi (Voice Over IP, VoIP) getirdiği avantajların yanında güvenlik açısından da bir takım zafiyetleri beraberinde getirmektedir. Bu makalede VoIP teknolojisini kullanarak yapılan ücret dolandırıcılıkları ve önleme yöntemleri incelenmiştir. Trafik yönlendirme, Servis sağlayıcı dolandırıcılığı ve sosyal mühendislik olmak üzere üç ana başlık halinde VoIP zafiyetleri ve önleme yöntemlerine değinilmektedir.

Anahtar Kelimeler: *VoIP, VoIP güvenliği, Siber Güvenlik, Ücret dolandırıcılığı, premiuım numaralar, arama yönlendirme*

Giriş

VoIP (Voice over Internet Protocol) teknolojisinin geleneksel ağlara kıyasla düşük maliyetle sağladığı gelişmiş hizmetler sayesinde kullanımı çok hızlı bir şekilde artmakta ve yaygınlaşmaktadır. VoIP paketlenmiş, dijital ses sinyallerinin, internet protokolü (IP) tabanlı ağlar üzerinden, gerçek zamanlı iletimi olarak ifade edilebilir. Fakat bu teknoloji ciddi güvenlik zafiyetlerini de beraberinde getirir.

Yetmişlerde, telekomünikasyon ağlarına uzaktan erişim olanaklarının artması ile beraber bu ağlar, yetkisiz ağ erişimi sağlamaya çalışan kişilerin hedefi haline gelmişti. Sesli posta ve sesli yönlendirme servislerinin kullanımı ile birlikte de ücret dolandırıcılığı (toll fraud) yeni bir telekomünikasyon sahtekârlığı olarak yaygınlaşmaya başladı.

Ücret dolandırıcılığı, en genel anlamda, telefon sistemlerinin yetkisiz kişilerce haksız gelir elde etme amacı güdülerek kullanılmasıdır. Bu dolandırıcılık türünde yapılan saldırı, telefon sistemlerinin, bilinmeyen kişiler tarafından ele geçirilip genellikle uzak mesafe ya da ücretli numaraya doğru yasa dışı bir çağrı yapılması ile gerçekleşmektedir.

Saldırgan ya da dolandırıcılar, küçük veya büyük şirketlerin iletişim sistemlerine güvenlik açıklarını kullanarak sızarlar ve saldırılarını gerçekleştirirler.

Geçmişte bu girişi yapmak için kullanılan en yaygın yöntem, özel santralin (Private Branch eXchange (PBX)) yönetim portunun ele geçirilmesi ile olmaktaydı, fakat günümüzde farklı pek çok şekilde bu saldırı gerçekleştirilebilmektedir.

Temel Bilgiler

Premium Numaralar: Arandığında sahibinin para kazandığı numaralar olmakla beraber Premium numara olarak adlandırılmaktadır. Premium numaralar halk arasında 900'lü hatlar olarak da bilinmektedir. Bu numaraları aramak yüksek ücretli oldukları için genel olarak dolandırma amaçlı kullanılmaktadır. Bu numaralara yönlendirilen arama trafiğinden kazanılan para yönlendirmeyi sağlayan saldırgan ile numara sahibi arasında paylaşılır.

Ücretsiz Hatlar (Toll Free): Halk arasında 800'lü hatlar olarak bilinmektedir. Arama aldığında hattın sahibi, Telekom şirketine ödeme yapmaktadır. Bu tür hatlar genel olarak şirketlerin çağrı merkezleri ya da müşteri ilişkileri departmanları tarafından kullanılmaktadır.

Konum Yönlendirme Numarası (Location Routing Number): Telekomünikasyon sistemine kayıtlı olan her telefonun servisinin kendine özel eşsiz bir numarası vardır. Bu numaralar tek bir çatı altında Toptan Sağlayıcı (Wholesale Provider) tarafından saklanmaktadır [2]. Servis sağlayıcıları bu numaraya ait eşsiz numara sayesinde, hat sahibine hizmet vermektedirler.

Telefon numarasının bağlı olduğu servis sağlayıcısını değiştirmeye yarayan hizmete Yerel Numara Taşınabilirliği (Local Number Portability (LNP)) denir.[2]

1. Ücret Dolandırıcılığı (Toll Fraud)

Telefon dolandırıcılığı telekomünikasyon sektöründe maddi kazanç sağlama amaçlı ücretlendirme sistemine yönelik gerçekleştirilen kötü niyetli aktivitelerdir. Bu aktivitelerin gerçekleştirilmesi sonucunda elde edilen karı dolandırıcı ve dolandırıcının aramaları yönlendirdiği kişi veya kişiler arasında paylaşılmaktadır. Bu saldırı tipi ile ilişkili detaylı raporlama CFCA (Communications Fraud Control Association) adlı kurum tarafından 2 yılda bir yapılmaktadır. CFCA'nın 2013 yılında uluslararası telekomünikasyon ücret dolandırıcılığı raporuna göre 43,6 milyar dolar para kaybı raporlanmıştır. CFCA'nın raporuna göre en popüler olan ücret dolandırıcılık çeşitleri raporda listelenmiştir.[1]

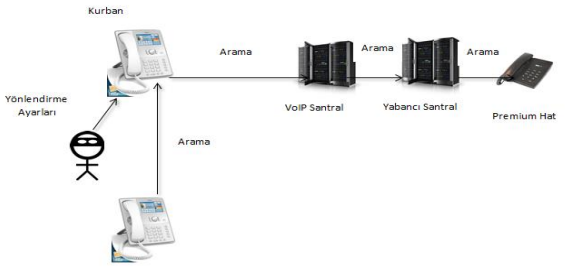
1.1 Hedefe Göre Telekom Dolandırıcılık Türleri

Dolandırıcılık türleri üç ana başlık altında toplanmaktadır. Bunlar VoIP Telekom Trafik Yönlendirme Dolandırıcılığı (Traffic Pumping Schemes), Servis Sağlayıcı Dolandırıcılığı (Schemes to Defraud Telecom Service Providers) ve Sosyal Mühendislik(Social Engineering) tir.

1.1.1 VoIP Telekom Trafik Yönlendirme Dolandırıcılığı Örnekleri

Trafik yönlendirme dolandırıcılığı, servis sağlayıcı trafiğinin yüksek ücretli hedeflere yönlendirilmesi ile olur. Yüksek ücretli trafiğin kullanılmasında ki amaç trafik kullanıcısına daha yüksek ücretler yansıtıp arada olan ücret farkının dolandırıcı ile servis sağlayıcısının paylaşması esasına dayanır. [2]

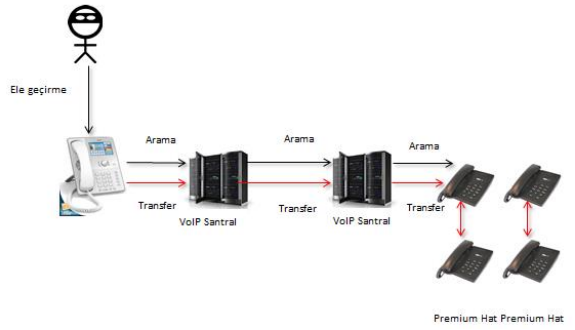
Arama Yönlendirme Dolandırıcılığı (Call Forwarding Fraud): Saldırgan sunucunun veya kullanıcının şifrelerini kırmak için Ortadaki Adam saldırısı (Man in the Middle Attack) veya Kaba Kuvvet Saldırısı (Brute Force) yapar. Şekil 1'de görüldüğü gibi, özel santral (Private Branch eXchange - PBX)e veya sesli yanıt sistemine (Interactive Voice Response) erişim sağlamaktadır. Erişilen sistemde kullanıcıların aramaları Premium hatlara yönlendirerek saldırı gerçekleştirilir. Gerçekleştirilen saldırıdaki zarar servis sağlayıcısının zafiyetinden kaynaklanıyor ise bu zarar servis sağlayıcısı tarafından karşılanabilir. Servis sağlayıcı bu zararı ödemeyi kabul etmeyebilir ya da bir kısmını itibar kaybetmemek amacı ile ödeyebilir [2].



Şekil 1. Arama Yönlendirme Dolandırıcılığı [2]

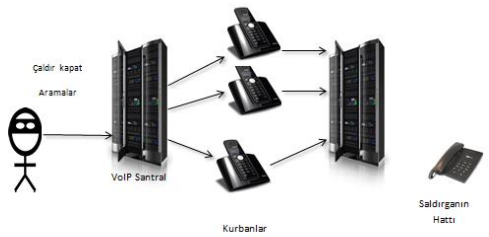
Çoklu Transfer Dolandırıcılığı (Multiple Transfer Fraud): Saldırgan arama yönlendirme dolandırıcılığında olduğu gibi kullanıcı şifrelerini kırıp bu kullanıcıların telefonlarını kullanarak Premium numaraları arayıp, aramayı bitirmeden aramaları kendi elindeki başka bir Premium numaraya transfer etmektedir. Telekom sistemlerinde transfer eden hat aramanın ücretini üstlendiği için, şifresi ele geçirilen kurban Premium numaralara yapılan çağrıların ücretlerini ödemek zorunda kalmaktadır.

Saldırgan tarafından başlatılan arama iki yüksek ücretli hat arasında devam ettirilerek konuşma ücreti arttırılır. Konuşma sırasında sürekli başka premium hatlara yönlendirilen bu aramalar daha büyük maddi kayıplar ile sonuçlanmaktadır.



Şekil 2: Çoklu Transfer Dolandırıcılığı [2]

Çaldır Kapat Dolandırıcılığı (One Ring and Cut (Wangiri) Fraud): Saldırgan, wangiri saldırı tipinde, hedef hattı bir kez arayıp açmasına fırsat vermeden kapatmaktadır. Şekil 3'te de görüldüğü gibi, saldırgan bu işlemi rastgele olarak birçok telefon kullanıcısına karşı gerçekleştirmektedir. Kullanıcıların telefonlarında görülen cevapsız çağrıyı masum olarak algılayıp geri aramaları sonucu bu aramaların premium numaralara yönlendirilmesi esasına dayanır.

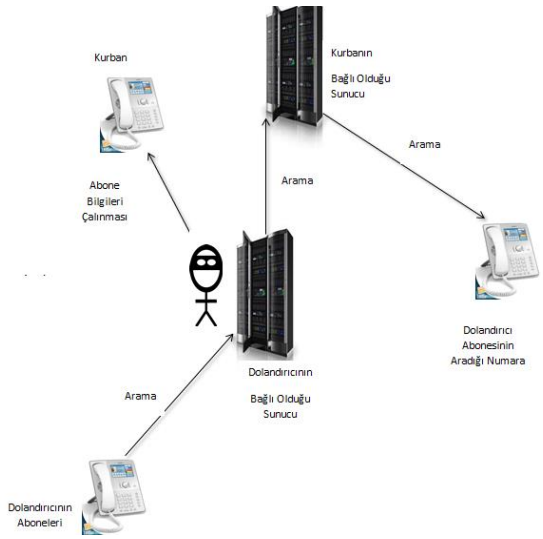


Şekil 3: Çaldır Kapat Dolandırıcılığı [2]

1.1.2 VoIP Telekom Servis Sağlayıcıları Dolandırıcılık Örnekleri

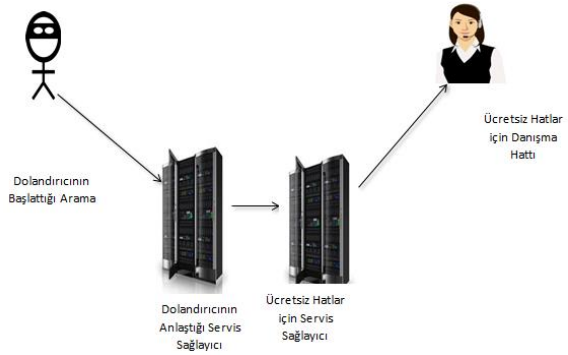
Dolandırıcılık saldırıları içinde en kapsamlı ve karmaşık olanıdır. Servis sağlayıcıların yasal boşluklarının saldırganlar tarafından fark edilip kötü amaçlı olarak kullanılmasıdır.

Toptan SIP Santrali Dolandırıcılığı (Wholesale SIP Trunking Fraud): Bu saldırı tipinde saldırgan bir servis sağlayıcının kullanıcı isimleri ve numaralarına ulaşmaktadır. Saldırgan kendisine SIP sunucusu kurup fazla kar elde edebileceğini düşündüğü kullanıcıları kendi kullanıcı listesine eklemektedir. Kayıtlı kullanıcılarından gelen aramaları, çalmış bulunduğu kullanıcı adları ve numaralarından gelen aramaları çağrıymış gibi göstererek, dolandırdığı servis sağlayıcı üzerinden aramayı gerçekleştirmektedir. Kendi kullanıcısından arama için para alırken gerçekte olarak aramanın ücretini bilgilerini çalmış olduğu kullanıcı ödemektedir. [2]



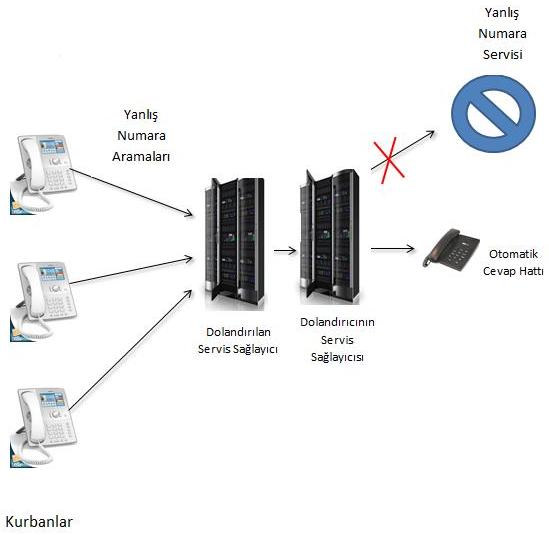
Şekil 4: Toptan SIP Santrali Dolandırıcılığı [2]

Ücretsiz Hatlar Dolandırıcılığı (Toll Free Fraud): Ücretsiz hatlar dolandırıcılığı ücretsiz olarak danışmanlık sağlayan bütün şirketleri etkileyebilir. Saldırgan ücretsiz arama yapılan numaraları arayıp uzun süre çağrıyı açık tutup ya da aynı anda fazla arama yaptırarak kurumsal şirkete yüksek ödeme yaptırabilir. Her aramada farklı numaralar kullanır ve aramaları iş saatleri içerisinde gerçekleştirir. Saldırgan sesli yanıt sistemini doğru bir şekilde yönlendirip çağrının uzun sürmesini sağlayabilir. Hedef şirketin kurumsal, büyük bir şirket olması bu saldırının fark edilmesini zorlaştırır. [2]



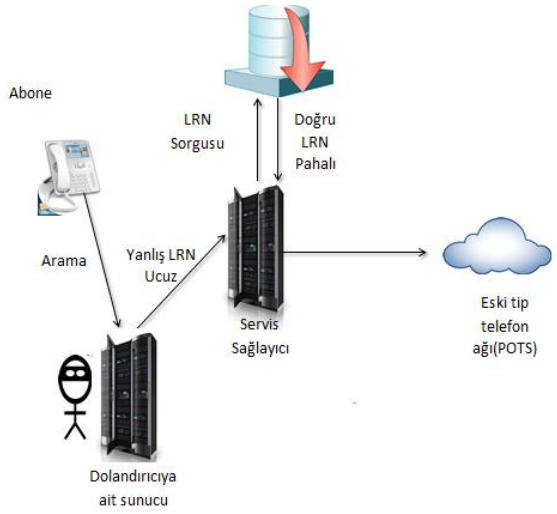
Şekil 5: Ücretsiz Hatlar Dolandırıcılığı [2]

Yanlış Cevap Denetimi (False Answer Supervision): Saldırgan arama rotası üzerinde konumlanmaktadır. Kullanıcılar yanlış numarayı aradıkları zaman normal koşullar altında arayan kişiye "Bu numara kullanımda değildir" şeklinde bir dönüş yapılır ve bu aramalarda arayan kişiden ücret talep edilmez. Saldırgan bu dönüş mesajını kullanarak arayan kişinin aramasını kendi elindeki, otomatik cevap verme özelliğine sahip bir hatta yönlendirir. Kullanıcının "Bu numara kullanımda değildir" sesli kaydını dinlemesi sürecinde saldırgan aslında aramanın elindeki hat tarafından cevaplanmış olmasını sağlar. Bu arama aramayı yapan kişi ve kullandığı tüm santrallere fatura edilir. Gerçekte arama sonlanmadığı için fatura edilecek bir durum bulunmamaktadır.



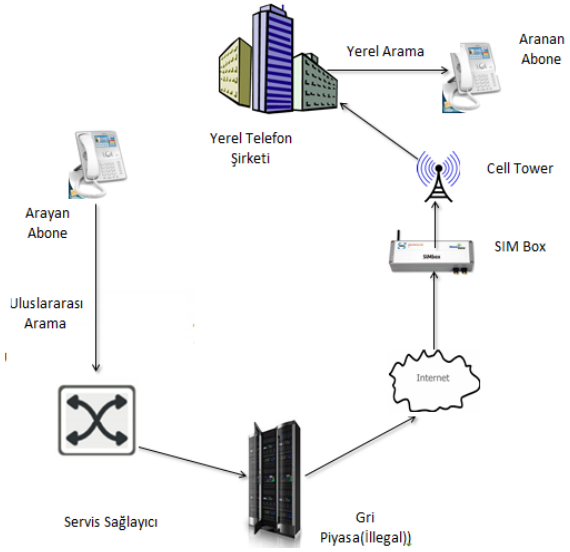
Şekil 6: Yanlış Cevap Denetimi [2]

Konum Yönlendirme Numarası Dolandırıcılığı (Location Routing Number Fraud): Normal bir arama başlatırken sunucular, aranan numaranın LRN'ı öğrenmek için ortak bir veri tabanından sorgulaması Şekil 7'de gösterilmiştir. Eğer SIP mesajı içindeki LRN daha önceden kayıtlı bir LRN ise ikinci kez sorgu atılmaz. Saldırgan bu noktada arama başlatırken ucuz bir LRN i SIP mesajı içerisine yerleştirir. Fakat saldırgan SIP mesajı içine yanlış LRN yazdığı için sunucu tekrar veri tabanına sorgu atar ve gerçekte pahalı olan bir LRN ı alır. Arayan kişi normalde pahalı bir LRN i aramasına rağmen bu sorgu için servis sağlayıcı masrafı öder. Arayan kişi ucuz olan LRN i verdiği için sadece bu kısmı ödemeye tabii olur.



Şekil 7: Konum Yönlendirme Numarası Dolandırıcılığı [2]

Toll Bypass Fraud: Bu saldırı servis sağlayıcılarının gerçekleştirdiği saldırı tipidir. Yasal kullanıcılar yurtdışı arama yapmak istediklerinde aramaların olması gerektiği gibi uluslararası servis sağlayıcılardan gitmesi gerekirken, saldırganların tasarladığı servis sağlayıcılara yönlendirilmesi ardından bu aramaların yerel arama gibi gösterilmesi ile aramanın daha ucuza yapılması ile gerçekleştirilir. Bu saldırı tipinde GSM Gateway Fraud veya SIM Boxing kullanılır. Şekil 8'de B2 rotasının takip edilmesi ile saldırı gerçekleştirilir.



Şekil 8: Toll Bypass Fraud [2]

Şekil 9: Yerel/Uluslararası Tarife Dolandırıcılığı [2]

1.1.3 Sosyal Mühendislik (Social Engineering)
Telefon dolandırıcılığı olarak bilinen en popüler saldırılardır.

Hesap Ele Geçirme (Account Takeover): Bu saldırı tipinde saldırgan genellikle finansal enstitüleri arayıp kendisini gerçek bir kullanıcı gibi gösterip kullanıcının hesap bilgilerine erişmeye çalışmaktadır.

Telekom Hizmetini Kullanım Dışı Bırakma (Telecom Denial of Service (TDOS)): Hizmet Dışı Bırakma (Denial Of Service) saldırıları gibi saldırgan çok fazla aramayı aynı anda yapması ve bu aramaları uzun sürdürmesi ile organizasyonun kapasitesini aşmasına sebep olur. Bu saldırı telekom şirketinin kullanıcıya hizmet vermesini olumsuz etkilemektedir. TDoS saldırılarını günümüzde toplumun genelini olumsuz etkilemektedir. Çünkü saldırgan hedef olarak hastaneleri, polis istasyonları gibi kamu kuruluşlarını seçmektedirler. [2]

Vishing (Voice Pishing): Pishing, saldırgan hedeflediği kişinin, kişisel veya banka bilgilerini çalma amacıyla yapılan saldırılardır. Vishing ise bu dolandırıcılığın telefon ile yapılmasıdır. Saldırgan kendisini legal bir kullanıcı gibi gösterip kamu hizmetleri sunan bir organizasyonu arar ve karşıdaki kişiyi bilgi toplayacak şekilde yönlendirir. Bu bilgileri kullanarak bilgilerini çaldığı kullanıcıyı arayıp kendisini bilgileri toplamak için kullandığı kamu organizasyonu gibi gösterip, kullanıcıyı dolandırır. [2]

2. Telefon Dolandırıcılık Saldırılarından Korunma Yöntemleri

[3]Ücret dolandırıcılığını (Toll Fraud) engellemek için konuşma kayıtlarının analiz edilmesi ile çözüme ulaşılabilir. VoIP sistemlerdeki konuşma kayıtları tutularak konuşmaların analiz edilmesi ile kötü niyetli olan VoIP katılımcıları tespit edilebilir. Bu analiz için sunucu ve istemciler arasındaki mesaj trafiği hem mesaj hacimleri hem de protokol parametreleri göz önüne alınarak incelenip akışın kötü amaçlı bir aktivite içerip içermediğine karar verilir. Örnek olarak normal trafik akışının çok üzerinde arama gerçekleşiyor ise bu arama girişimleri Hizmet Dışı Bırakma saldırısı olarak adlandırılabilir. Bu durumda sistem yöneticilerine uyarı verilir ve bu uyarılar kayıt altına alınır.

VoIP sistemini yazılımsal ve donanımsal olarak yapılandırmak ile birlikte sistem yetkilisinin kararları çözüm önerilerinin bir parçası olmaktadır. VoIP katılımcıları kara liste, beyaz liste ve gri liste olmak üzere üçe ayrılmıştır. Bu üç liste Saldırı Sezme Sistemi(Intrusion Detection System (IDS)) ne gelen giden çağrılar girdi olarak alınıp doldurulmaktadır. Saldırı Sezme Sistemi, sisteme karşın tehlikeli ve şüpheli olan davranışları kayıtlar. Teknolojik olarak dünya üzerinde bilinen ve daha önceden kaydedilmiş saldırı tipleri saldırı veri tabanlarında toplanır. Kullandığımız IDS sistemleri bu veri tabanlarını sürekli olarak güncel tutar ve sunuculara gelecek saldırıların sürekli izlenebilmesini sağlar. Saldırı Sezme Sistemi, sadece analiz ve izleme sistemleridir. Herhangi bir engelleme özellikleri bulunmamaktadır [5]. Saldırı sezme sistemlerine girdi olarak alınan arama kayıtları daha sonra Arama Detay Kayıt Analiz Sistemlerine(CDRAS) girdi olarak alınıp bu çağrılar beyaz, kara veya gri listeye alınmaktadır. [3]

Ele alınan çözüm önerilerinde kullanıcı gizliliğini korumak amaçlı Adil Bilgi Uygulama Prensibi (Fair Information Practices Principles (FIPP)) kabul edilmiştir. Bu amaçla çağrı kayıtları (Call Detail Record (CDR)) analiz edilirken dikkat edilen hususlar şunlardır [3]:

- Çağrı kayıtları içindeki veriler gizli tutulmalı,
- Çağrı kayıtları kurallarda belirtildiği şekilde saklanılmalı,
- Çağrı kayıtları içindeki kullanıcı bilgilerinin ne amaçlı nerede kullanılacağı konusunda kullanıcı bilgilendirilmeli,
- Veri analizi yapıldıktan sonra veriler silinmelidir.

Bu saldırılar için yaklaşımlar;

Arama Detay Kayıt Analiz Sistemi (CDRAS) olarak adlandırılan sistemde, bahsi geçen kara, beyaz, gri listelerin oluşturulması; çağrı kayıtlarından elde edilen arama istek süresi, arama süresi ve aranan kişiye aramanın ulaşma süresi temel alınarak elde edilir. Beyaz liste geçerli olan VoIP katılımcılarını, kara liste kötü niyetli VoIP katılımcılarını, gri liste ise yetkili kişiye gönderilip kötü niyetli olup olmadığının yetkili kişi tarafından kontrol edilmesi gereken VoIP katılımcılarını göstermektedir. Geçmişteki arama verileri ile güncel arama verilerinin karşılaştırılması ile listeler oluşturulmaktadır. CDRAS; IDS SNORT ile birlikte kullanılarak VoIP saldırılarına karşın etkin görev alabilir. SNORT açık kaynak kodlu saldırı tespit ve engelleme sistemi yazılımı olmakla birlikte yaygın olarak kullanılan saldırı tespit sistemlerinden biridir. Genel olarak imza tabanlı olarak çalışan SNORT, protokol ve anomali analizi yapabilme yeteneğine de sahiptir. SNORT ile farkı CDRAS nin davranıştan öğrenme tabanlı çalışmasıdır.[4] CDRAS yaklaşımındaki yanlış pozitif(false positive) oranının

düşürülmesi için yeni eşik değerleri tanımlanmıştır.[3]

Özel santral (Private Branch eXchange (PBX)) saldırısı için alınabilecek önlemler sırasıyla şunlardır; telefon sistem yetkililerinin güvenlik prosedürlerinin sıkıştırılması, çalışanların daha karmaşık şifreler kullanmaya teşvik edilmesidir. Ayrıca organizasyona göre uluslararası aramaların kapatılması da önlem olarak alınabilir.

Yanlış Cevap Denetimi (False Answer Supervision) dolandırıcılığı için alınabilecek önlemler sırasıyla şunlardır; arama süresinin 5-10 saniye sürdüğü aramaların raporlanması, yasal olan arama sürelerinin kayıt altına alınması ve bu aramalar ile toplanan verilerin karşılaştırılması ve sahte olan aramaların belirlenmesi sayılabilir.

Uluslararası Gelir Payı Dolandırıcılığı (International Revenue Share Fraud (IRSF)) önlemek için alınabilecek önlemler sırasıyla şunlardır; premium hatların listelerinin tutulması ve bu liste içinde sürekli aramaların yönlendirildiği hatların tespit edilmesi, premium hatlara yönlendirilen arama sürelerinin tespit edilmesi ve normal süreden uzun süren aramaların durdurulması yöntemleri izlenebil-mektedir.

Sonuç

Bu makalede, VoIP telekom trafik yönlendirme dolandırıcılıkları, VoIP telekom servis sağlayıcıları dolandırıcılıkları ve sosyal mühendislikle gerçekleştirilen dolandırıcılık türleri için çeşitli çözüm önerileri sunulmuştur. Bu çözüm önerileri genel olarak konuşma kayıtlarının ayrıntılı bir şekilde tutulup analiz edilmesi temeline dayanmakta olup her bir kullanıcı için geçmişteki ve günümüzdeki detaylı konuşma kayıtları incelenmektedir. Son olarak da alınabilecek genel tedbirler çerçevesinde: uluslararası aramaların engellenmesi, VoIP kullanıcılarının telekomünikasyon sistemlerine olan erişimlerini sağlayan şifrelerin güçlü olmasının teşvik edilmesi ve premium hatların listesinin tutulması önerileri sunulmuştur.

Reference

[1] Communications Fraud Control Association, Global Report, 2013

[2] TELECOM FRAUD CALL SCENARIOS by TransNexus-http://transnexus.com/wp-content/uploads/TFS.pdf

[3] Beckers, K. ; Quirchmayr, G. ; Sorge, C, "A Lightweight Privacy Preserving Approach for Analyzing Communication Records to Prevent VoIP Attacks using Toll Fraud as an Example" IEEE, 2012

[4]B. Dayıoğlu "SNORT ile Saldırı Tespiti", 2003

[5] SIP Intrusion Detection and Prevention: Recommendations and Prototype Implementation S. Niccolini A, R. G. Garroppo B, S. Giordano B, G. Risi B, S. Ventura C