PoS Sistemlerine Yönelik RAM Kazıma Saldırılarının İstatistiksel Analizi ve Savunma Önerileri

Ecir Uğur Küçüksille, Bekir Eray Katı, Mehmet Ali Yalçınkaya

***Özet*— Kredi kartlarının yaygınlaşması ile birlikte PoS (Point of Sale) cihazları neredeyse bütün endüstriyel sektörlerde yaygın olarak kullanılmaya başlanmıştır. Kredi kartlarının kullanımın bu kadar yaygınlaşması, söz konusu kartlara ait verilerin elde edilmesi amacıyla gerçekleştirilen saldırılarda da doğru orantılı olarak artış meydana getirmiştir. Bu çalışmada kredi kartlarına ait verilerin elde edilebilmesi amacıyla gerçekleştirilen RAM kazıma saldırıları incelenerek, kurum ve kuruşlara söz konusu saldırılara karşı alınabilecek önlemler sunulmuştur. Ayrıca RAM kazıma saldırılarında kullanılan zararlı yazılımlar incelenmiş, söz konusu saldırıların farklı sektörlerde yıllara göre neden olduğu zararlar, araştırma raporlarından elde edilen istatistiki veriler ışığında analiz edilmiştir. Gerçekleştirilen çalışma RAM kazıma saldırılarına derinlemesine bir bakış sunarak, söz konusu saldırıların etkilerini minimuma indirmek adına çözümler sunmaktadır**

Anahtar Kelimeler— PoS, Kredi Kartı, RAM Kazıma, Track, REG-EX Algoritması, Luhn Algoritması.

***Abstract*— With the expansion of credit cards, PoS devices have been used widely almost in all industrial sectors. Because of the widespread usage of credit cards, RAM scraping attacks which are performing in order to obtain data from said card, increased proportionally. In this study, we investigated the RAM scraping attacks that carried in order to obtain credit card data and we present different defense methods for companies to prevent these attacks. Also we examined malwares used in these attacks and damages caused in different sectors many years examined making use of the statistical data that obtained from research reports. This study provides an in-depth overview to RAM scraping attacks and offers solutions in order to minimize the effects of such attacks.**

Keywords— PoS, Credit Card, RAM Scraping, Track, REG-EX Algorithm, Luhn Algorithm.

E.U. Küçüksille, Süleyman Demirel Üniversitesi Bilgisayar Mühendisliği Bölümü, Merkez, Isparta, Türkiye; (telefon: +90(246)2111478;e-posta: ecirkucuksille@sdu.edu.tr)

B.E. Katı, Süleyman Demirel Üniversitesi Bilgisayar Mühendisliği Bölümü, Merkez, Isparta, Türkiye (telefon: +90(537)5715271; e-posta: bekireraykati@gmail.com)

M.A. Yalçınkaya, Süleyman Demirel Üniversitesi Bilgisayar Mühendisliği Bölümü, Merkez, Isparta, Türkiye (telefon: +90(246)2111381; e-posta: mehmetyalcinkaya@sdu.edu.tr)

I. GİRİŞ

Günümüzde gerek gerçek hayatta gerekse sanal ortamda kredi kartlarının kullanım alanı oldukça yaygınlaşmıştır. İnsanlar beraberlerinde yüklü miktarda nakit para taşımak yerine bankamatik veya kredi kartı taşımayı tercih etmektedirler. Kredi kartlarının giderek yaygınlaşması, söz konusu kartları ve kartlar ile alışveriş işlemlerinde kullanılan diğer sistemleri açık birer hedef haline getirmiştir. Saldırganlar gerçekleştirdikleri saldırılarda, tüketiciler tarafından kullanılan kredi kartlarına ait verileri ele geçirmeyi amaçlamaktadır. Bu amaçla gerçekleştirilen RAM kazıma saldırılarında saldırganlar, kredi kartları ile gerçekleştirilen alışveriş işlemlerinde kullanılan PoS cihazlarının bağlı olduğu sunucuları hedef almakta ve birçok kredi kartı kullanıcısının track (manyetik bant verisi) bilgilerini ele geçirmektedir.

Uluslararası akademik dünyada RAM kazıma saldırıları konusunda yapılmış çeşitli çalışmalar mevcuttur. Fakat ülkemizde henüz POS cihazlarına yönelik gerçekleştirilen RAM kazıma saldırılarını inceleyen bir çalışma bulunmamaktadır. Literatürde yer alan yabancı kaynaklı çalışmalar incelendiğinde söz konusu çalışmaların RAM kazıma saldırılarının metodolojisi ve etkilerini detaylı olarak incelediği görülmektedir. Gerçekleştirilmiş olan bu çalışmanın literatürde yer alan diğer çalışmalardan farkı ise, RAM kazıma saldırıları konusunda, çeşitli araştırma raporlarından elde edilen en güncel istatistiksel verilerin toplanmış olması, böylelikle de söz konusu saldırıların tarihsel gelişimi, işletim sistemlerine göre görülme oranları, ülkelere göre görülme oranları, farklı endüstriyel alanlarda görülme oranları ve bu oranların yıllara göre değişimi gibi konularda istatistiksel bir bakış açısı sunmasıdır.

Bu çalışmada 2.Bölümde RAM kazıma saldırılarının genel metodolojisinin yanı sıra kredi kartlarına ait verilerin saklandığı çeşitli veri grup formatlarına değinilmiştir. Bu bölümde ayrıca RAM kazıma saldırılarında, saldırganların kredi kartlarına ait verileri elde etmek için kullandıkları çeşitli algoritmalara değinilmiştir. 3. Bölümde saldırganların RAM

kazıma saldırılarında izledikleri saldırı senaryolarına değinilmiş ve RAM kazıma saldırılarının işletim sistemlerine göre gerçekleşme oranları incelenmiştir. 4.Bölümde saldırganlar tarafından RAM kazıma saldırılarında kullanılan zararlı yazılımların tarihsel gelişimi ve işleyişi incelenmiştir. Gerçekleştirilen çalışmanın 5. Bölümünde, POS cihazlara yönelik gerçekleştirilen RAM kazıma saldırılarının diğer saldırılara oranı ve söz konusu saldırıların ülkesel olarak dağılımı, ülkemizde gerçekleşmiş örnekleri sunularak, istatistiksel grafiklerle incelenmiştir. Gerçekleştirilen çalışmanın 6. Bölümünde RAM kazıma saldırılarına yönelik alınabilecek önlemler sunulmuş, 7. Bölümde ise gerçekleştirilen saldırıların sonuçlarına değinilmiştir.

II. RAM KAZIMA SALDIRILARININ METODOLOJİSİ VE KREDİ KARTI BİLGİLERİNİN ELE GEÇİRİLMESİ

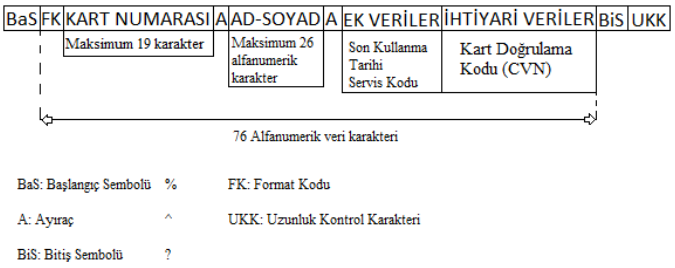
RAM kazıma saldırılarında, kredi kartıyla PoS cihazı kullanılarak bir işlem yapıldığında kart verileri öncelikle şifrelenmiş bir şekilde sunuculara iletilmektedir. Ödeme doğrulama aşamasında şifrelenmiş olan bu veriler çözümlenerek, sunucuda bulunan RAM üzerinde çok kısa bir süreliğine tutulmaktadır. PoS sunucusu üzerine, saldırganlar tarafından çeşitli saldırı metotları aracılığı ile yerleştirilen RAM kazıyıcı zararlı yazılımlar, RAM üzerinde tutulan bu kredi kartı verilerini çeşitli algoritmaları kullanarak tespit etmektedir. Elde edilen bu veriler içinde kart numarası, kullanıcı adları, adresler, söz konusu kartın son kullanım tarihi ve kart doğrulama kodu (CVN) gibi verileri barındıran Track veri grupları bulunmaktadır [1]. Gerçekleştirilen saldırıların ve elde edilen verilerin daha anlaşılır olması açısından kredi kartlarında kullanılan çeşitli veri kayıt tiplerine değinmek gerekmektedir.

Manyetik şerite sahip kredi kartlarında Track adı verilen 3 farklı veri grupları tutulabilir. Bu çalışma kapsamında incelenmiş olan ödeme amaçlı kullanılan kartlarda, Track 1 ve Track 2 veri grupları tutulmaktadır. Bu veri grupları Uluslararası Standartlar Teşkilâtı (ISO) ve Uluslararası Elektroteknik Kurulu (IEC) tarafından standart hale getirilmiştir [2].

Track 1 veri grubu ilk olarak Uluslararası Hava Taşıma Birliği (IATA) tarafından oluşturulmuştur. Track 1 veri grubunu kullanan kartlarda manyetik şerit üzerinde 79 alfa numerik karakter içeren 210 bit veri depolanabilmektedir.

Track 2 veri grubu ise Amerikan Bankacılar Birliği (ABA) tarafından oluşturulmuştur. Track 2 veri grubunu içeren kartlarda manyetik şerit üzerinde 40 alfa numerik karakter içeren 75 bit veri depolanabilmektedir [3]. Şekil 1' de Track 1 veri grubu formatları gösterilmektedir.

Kredi kartlarında ayrıca 3 veya 4 haneli olan CVN bulunmaktadır. Kart doğrulama kodu, kredi kartı markasına göre CAV, CID, CVC, CVV şeklinde isimlendirilebilmektedir. 1 Ocak 1997'den itibaren tüm Mastercard'larda, 1 Ocak 2001'den itibaren de tüm Visa'larda güvenlik kodu bulunması zorunlu hale gelmiştir. Kart basımı sırasında kart numarası ve kartın son kullanma tarihi bankanın belirlediği bir algoritmadan geçirilerek güvenlik numarası oluşturulmaktadır. Her kart için bu numaralardan 2 adet üretilmektedir. Bunların bir tanesi (CVV) manyetik bant içindeki Track veri grubu içerisinde saklanırken, diğeri (CVV2) genellikle kartın arka yüzeyinde imza bandının olduğu yerde bulunmaktadır. CVV2 numarası sanal harcamalarda kartı fiziksel olarak doğrulamak için kullanılmaktadır [4].

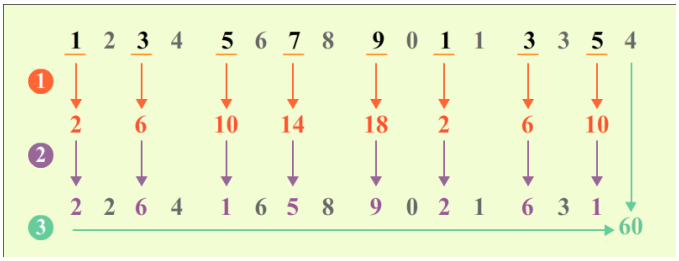


Şekil 1: Track1 veri grubu formatı

RAM kazıma saldırıların POS sunucularına saldırganlar tarafından çeşitli yöntemler ile yerleştirilmiş olan zararlı yazılımlar, RAM üzerinde yer alan kart numarasını ararken REG-EX (Regular-Expression) algoritmasını kullanmaktadırlar. Günümüzde kredi kartı numarasını doğrulamak için kullanılan olan ilk algoritma REG-EX algoritmasıdır. Her bir kredi kartı, kendi finansal şirketinin belirledikleri kurallar çerçevesinde bir kart numarasına sahiptir. Söz konusu kart numarasının uzunluğu 13 ile 16 karakter aralığındadır. İlk 4 hane kredi kartı türlerinin birbirinden ayırt edilmesinde kullanılmaktadır [5]. Regex algoritmasının işleyişine değinmeden önce farklı kart türlerine ait kart numaralarına değinmek gerekmektedir. Visa tipi kartlarda, kart numaraları her zaman 4 ile başlamaktadır. Daha sonra gelecek olan 12 adet rakam ise 0 ile 9 arasındaki rakamlardan oluşmaktadır. MasterCard tipi kartlarda tanımlı kart numaralarının ilk 2 hanesi 51 ile 55 arasındaki sayılardan oluşmaktadır. Geri kalan 14 hane ise 0 ile 9 arasındaki rakamlardan oluşmaktadır. Söz konusu kartlarda kart numarası toplamda 16 haneden oluşmaktadır. American Express tipi kartarda kart numarası 34 veya 37 ile başlamaktadır. Geri kalan 13 hane ise 0 ile 9 arasındaki rakamlardan oluşmaktadır. American Expres tipi kartlarda kart numaraları toplamda 14 haneye sahiptir.

Saldırganlar bahsedilen tiplerdeki kart numaralarını tespit edebilmek için REG-EX algoritmasını kullanmaktadır. Söz konusu algoritma kullanılarak gerçekleştirilen arama işlemlerinde, iki adet \b tagı arasına kart tipine ait tanımlama yerleştirilerek arama gerçekleştirilmektedir. *Realgoritması* kullanılarak Visa tipindeki bir karta ait kart numarasının tespit edilebilmesi için "\b4[0-9]{12}(?:[0-9]{3})?\b" bloğu kullanılmaktadır. Söz konusu blokta "\4" ifadesinden sonra yer alan "4" ifadesi, aratılacak kart numarasının ilk hanesinin, 4 olduğunu, "[0-9]{12}" ifadesi ise daha sonra gelen 12 rakamın

0 ile 9 arasındaki rakamlardan oluştuğunu belirtmektedir. Saldırganlar gerçekleştirdikleri aramalarda söz konusu bloğu, ilgili kart tipine göre değiştirerek, kart numarasını elde etmeyi amaçlamaktadırlar. Gerçekleştirilen RAM kazıma saldırılarında, kredi kartı numarasının tam olarak tespit edilmesinde regex algoritması tek başına yeterli değildir. Çünkü RAM' den kazınan verileri içerisinde geçersiz verilerde bulunabilmektedir. Saldırganlar regex algoritmasını kullanarak elde etmiş oldukları verilerin doğruluğunu onaylamak için Luhn Algoritması kullanmaktadırlar. Tespit edilen kart numaralarının Luhn algoritması kullanılarak geçerliliğinin doğrulanması işlemi Şekil 2' de gösterilmektedir.



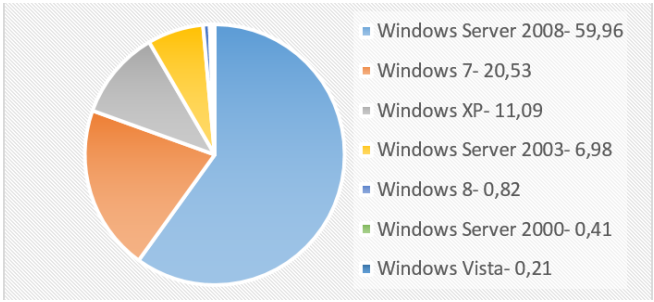
Şekil 2: Kredi kartları için kullanılan Luhn algoritmasının gösterimi [6]

Luhn algoritması kullanılarak elde edilen kart numarasının doğrulanması işleminde ilk olarak, kart numarasında tek haneye denk gelen sayılar 2 ile çarpılmaktadır. Eğer elde edilen sonuç 2 basamaklı bir sayı ise, söz konusu sayının rakamları toplanmaktadır. Eğer elde edilen sonuç tek rakamlı ise, olduğu gibi bırakılmaktadır. Son olarak tespit edilen kart numarasında çift haneye denk gelen rakamlar ile birlikte, bir önceki adımdan elde edilen sonuçlar toplanmaktadır. Gerçekleştirilen tüm işlemler sonunda elde edilen toplam sonuç 10'a tam bölünebiliyorsa, RAM' den kazınmış olan kart numarası Luhn algoritmasına göre geçerli bir kart numarasıdır [6].

III. RAM KAZIMA SALDIRI KAYNAKLARI

Saldırganlar tarafından gerçekleştirilen RAM kazıma saldırılarında, şirket içi, sosyal mühendislik ve oltalama gibi birçok saldırı kaynağı bulunmaktadır. Söz konusu saldırı kaynaklarından ilki şirket içinden gerçekleştirilen saldırılardır. Şirket içinden gerçekleşecek bir saldırı, savunulması en güç saldırı türüdür. Şirket içinde çalışan kötü niyetli kişilerin doğrudan sistem sunucularına yazılımsal veya donanımsal olarak erişebilmesi mümkündür. RAM kazıma amacıyla kullanılacak zararlı yazılım, bir USB aracılığıyla kolaylıkla sunucu yazılımına bulaştırılabilir.

RAM kazıma saldırılarında karşılaşılan diğer saldırı kaynakları da yemleme ve sosyal mühendisliktir. Saldırganlar şirket içinde çalışan yetkili kişilere e-posta yolu ile ulaşarak şirket içerisinde yer alan sistemlere zararlı yazılımlar bulaştırabilmektedir. Söz konusu saldırı türünde çoğunlukla kendisini bir banka yetkilisi olarak tanıtan bir saldırgan, şirket içinde yer alan çalışana sahte bir mail göndermektedir. Bu mail içerisinde, eklenmiş zararlı bir yazılım ya da zararlı yazılımı barındıran, kurbandan tıklaması istenen bir link içermektedir. Mail ekindeki ya da gönderilen linkteki zararlı yazılımın indirilip çalıştırılması ile saldırganlar, şirket iç ağında yer alan bir sistem üzerinde oturum elde edebilmektedir. Oturum elde edilen bu sistem, küçük boyuttaki bir şirkette yetersiz kaynaklardan dolayı hem kişisel bilgisayar hem de PoS sunucu olarak hizmet veriyor olabilir. Böyle bir durumda saldırgan doğrudan PoS sunucuya erişim sağlamış olmaktadır [7]. Büyük boyuttaki şirketlerde ise PoS sunucu olarak hizmet veren sistemler, kullanıcılara ait sistemlerden ayrı tutulmaktadır. Bu tarz durumlarda saldırganlar, oturum elde etmiş oldukları şirket iç ağındaki bir sistemden, ağ pivotlama (network pivoting) işlemi ile şirket içerisinde yer alan PoS sunuculara erişim sağlayabilmektedir.



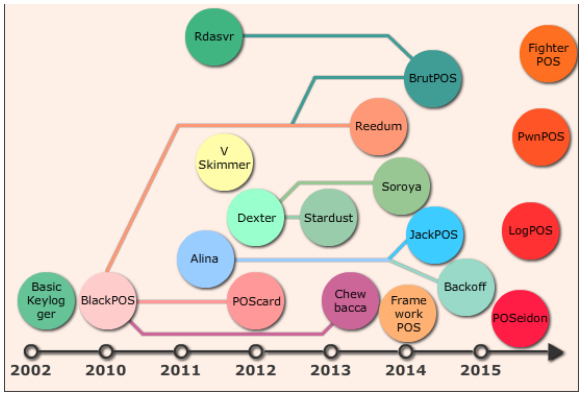
Şekil 3: Yapılan RAM kazıma saldırılarının işletim sistemine göre dağılımı [8]

Ayrıca günümüzde kurumlar tarafından kullanılmakta olan birçok yazılımda veya işletim sisteminde güvenlik açıkları bulunmaktadır. Bu güvenlik açıkları gerek yazılım test uzmanları, gerekse kullanıcı geri bildirimleriyle incelenip uygun güncelleştirmeler ile giderilmektedir. Kurum içerisinde kullanılan yazılım ve işletim sistemlerinin sürekli olarak güncel tutulması, PoS saldırılarına karşı hayati önlem taşımaktadır. Şekil 3' te bugüne kadar gerçekleştirilmiş RAM kazıma saldırılarının işletim sistemlerine göre oranları verilmiştir. Söz konusu grafik incelendiğinde, toplam saldırıların neredeyse %60' ının Windows Server 2008 işletim sisteminin kullanıldığı sunuculara yönelik olarak gerçekleştiği görülmektedir [8], [9].

IV. RAM KAZIMA SALDIRINDA KULLANILAN ZARARLI YAZILIMLAR

Kredi kartı kullanımı ve PoS sistemlerinin yeni yeni yaygınlaşmaya başladığı yıllarda saldırganlar basit keyloggerlar kullanarak tek bir hedef cihaz üzerine çeşitli saldırılar gerçekleştirmişlerdir. Gelişen teknoloji ile birlikte kredi kartları ve PoS cihazları için köklü güvenlik değişimlerine gidildiğinden dolayı saldırganlar, güvenlik önlemlerini aşmak için yeni yollar aramaya, yeni yazılımlar geliştirmeye başlamışlardır. Bu bölümde PoS cihazlara yönelik RAM kazıma saldırılarında kullanılan zararlı yazılımlar incelenmiştir. 2012 yılına kadar PoS sunucularına yönelik

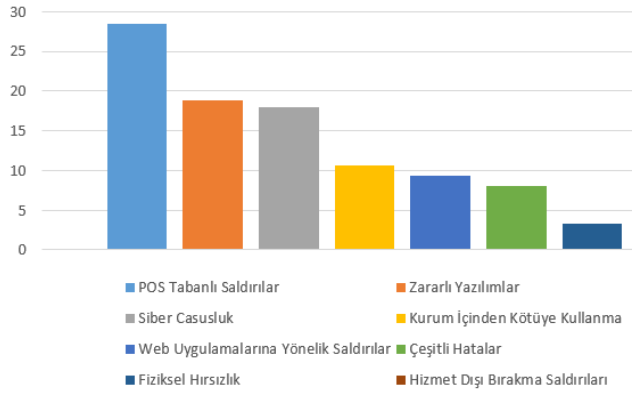
olarak gerçekleştirilen büyük çaplı saldırılarda BlackPOS isimli zararlı yazılım rol almıştır. BlackPOS, 2010 yılında Rus hacker Sergey Taraspov tarafından geliştirilmiştir. Söz konusu zararlı yazılım, indirildiği sistem üzerinde yer alan bellek içerisindeki kart verilerini tespit etmektedir. Söz konusu arama işleminde BlackPOS, bir önceki başlık altında incelenmiş olan arama ve doğrulama algoritmaları yardımı ile eş zamanlı olarak hem kredi kartı bilgisine uygun olabilecek tüm verileri taramakta hem de bulduğu verilerin geçerliliğini test etmektedir. BlackPOS aynı zamanda, söz konusu bellekten elde ettiği ek verileri, ilerleyen süreçte çevrimdışı ortamda inceleyip filtrelemek amacıyla depolayabilmektedir. PoS sunuculara yönelik gerçekleştirilen saldırıların büyük kısmında etkin olarak kullanılan BlackPOS, diğer PoS zararlı yazılımlarının geliştirilmesinde önemli bir paya sahiptir [10]. BlackPOS zararlı yazılımının geliştirilmesi ile elde edilen POSCard, Chewbacca, Reedum ve BrutPOS zararlı yazılımları 2012 ve 2015 yılları arasında gerçekleştirilen saldırılarda etkin bir şekilde kullanılmıştır. Şekil 4' te RAM kazıma saldırılarında kullanılan zararlı yazılımların zamana bağlı oluşum grafiği ve söz konusu zararlı yazılımlar arasındaki ilişkiler gösterilmektedir.



Şekil 4: RAM kazıma saldırılarında kullanılan zararlı yazılımların tarihsel gelişimi [10]

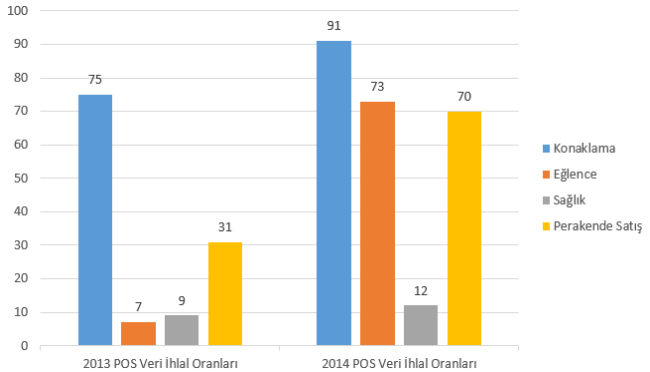
V. İSTATİSTİKSEL VERİLER İLE RAM KAZIMA SALDIRILARININ ETKİLERİNİN İNCELENMESİ

BlackPOS zararlı yazılımı kullanılarak gerçekleştirilen saldırılar sonrasında büyük firmalar hem maddi hem de prestij olarak ciddi zarara uğramışlardır. Bunun üzerine 2012 yılından itibaren PoS sistemlerin güvenliklerinin sağlanması, temel güvenlik politikaları içerisinde en önemli maddelerden biri haline gelmiştir ve söz konusu saldırıların neden olduğu risk değeri istenilen seviyelere düşürülmüştür. Bu düşük orana rağmen, Verizon 2015 veri ihlal raporuna göre, günümüz siber dünyasında gerçekleştirilen veri istismarı saldırıları içerisinde en büyük pay, 28.5% oranla PoS sunuculara yönelik saldırılardır. Elde edilen bu oran saldırganlar açısından kredi kartı verilerinin ne kadar değerli olduğunun önemini göstermenin yanı sıra, PoS sunuculara yönelik saldırıların neden olduğu kayıpları ispatlar niteliktedir. Şekil 5'te 2015 yılında gerçekleştirilen saldırı türleri ve oranları gösterilmektedir [11].



Şekil 5: 2015 yılı veri istismarı saldırı sınıflarının görülme oranları [11]

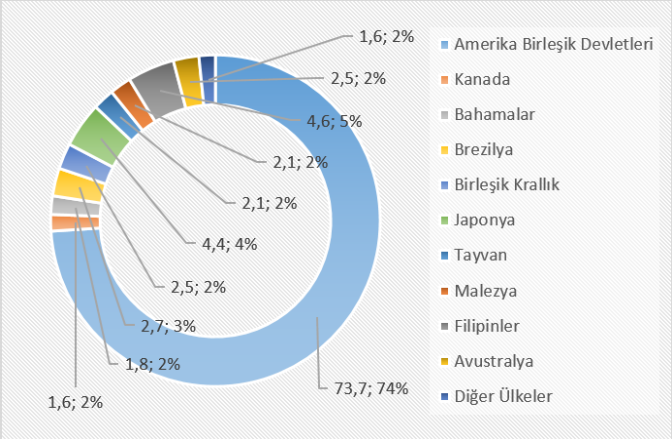
Kredi kartları günlük hayatta bireylerin alışveriş, konaklama, eğlence ve sağlık gibi birçok ihtiyacın karşılanmasında yardımcı olmaktadır. PoS sistemlerine yönelik gerçekleştirilen RAM kazıma saldırılarında saldırganlar çoğunlukla konaklama, eğlence, sağlık ve perakende satış gibi endüstriyel sektörlerde hizmet veren firmalar hedef alınmaktadır. Araştırma raporlarından elde edilen veriler incelendiğinde, 2013 yılında söz konusu alanlar içerisinde en fazla saldırıya konaklama sektöründe hizmet veren firmalar uğramıştır. 2014 yılında gerçekleştirilen saldırılarda ise yine en fazla konaklama sektörü hedef alınırken, perakende satış ve eğlence sektörlerinde hizmet veren firmalara yönelik saldırılarda büyük artış gözlemlenmiştir. Şekil 6' da 2013 ve 2014 yıllarında konaklama, eğlence, perakende satış ve sağlık sektörüne yönelik gerçekleştirilen RAM kazıma saldırılarının artış yüzdeleri gösterilmektedir [11].



Şekil 6: 2013 ve 2014 yıllarındaki endüstriyel alanlarda gözlemlen0ne RAM kazıma saldırılarının artış yüzdesinin gösterimi [11]

Gerçekleştirilen saldırılarda çoğunlukla insan hayatı için zorunlu ihtiyaç veren sektörler hedef alındığından dolayı, birçok dünya ülkesi RAM kazıma saldırılarına maruz

kalınmıştır. Şekil 7' de RAM kazıma saldırılarının ülkesel olarak dağılımı gösterilmektedir. Söz konusu şekilde görüldüğü gibi Amerika Birleşik Devletleri, gerçekleştirilen RAM kazıma saldırılarına maruz kalmada en yüksek paya sahiptir. Bu yüksek saldırı oranının en temel sebeplerinden biri, yüksek ekonomiden kaynaklanan pahalı malların alım satım oranının diğer ülkelere göre daha yüksek olmasıdır [12].



Şekil 7: PoS RAM kazıma saldırılarının ülkesel dağılımı [12]

Ülkemizde PoS sistemlere yönelik gerçekleştirilen RAM kazıma saldırılarından en önemlisinde, 2006 yılında GİMA Ticaret AŞ'ne 8 ile 22 Mayıs tarihleri arasında kredi kartı kullanarak alışveriş yapan müşterilerin kart bilgileri kopyalanmıştır [13]. Bankalar, bilgileri kopyalanmış olan kredi kartlarında anormal harcama değerleri tespit etmişlerdir. Gerçekleştirilen bu saldırı sonrasında Türkiye'deki kartlı ödeme sisteminde köklü bir çözüme gidilmiştir. Çipli kredi kartlarının üretilmesiyle, kartların sadece PoS cihazına okutulması zorunlu hale getirilmiştir. PoS cihazlarına bağlı bulunan kart pini giriş sistemi sayesinde bilgiler PoS üzerinde şifrelenip bankaya şifreli bir şekilde gönderilmeye başlanmıştır [14].

ABD ve bazı ülkelerde bankacılık ve ödeme sistemi ülkemizden farklıdır. Bu ülkelerde çipli kart sistemi yaygın olarak kullanılmadığı için PoS cihazı yerine bilgisayar üzerinde kullanılan PoS uygulaması kullanılmaktadır. Söz konusu uygulamada savunma düzeyi donanım katmanından uygulama katmanına geçtiği için saldırganlar tarafından daha rahat istismar edilmektedir. Visa Veri Güvenliği raporuna göre 2 Ekim 2008'de yaptığı uyarıda ABD'nin birçok bölgesinde geniş çaplı saldırıların gerçekleştirileceğini belirtmiştir. 2014 Ocak ayında ise gerçekleştirilen saldırılardan en çok etkilenen Target firmasının yaklaşık 70 milyon müşterisine ait kredi kartı verileri saldırganlar tarafından ele geçirilmiştir [15].

VI. POS SİSTEMLERE YÖNELİK RAM KAZIMA SALDIRILARINA KARŞI ALINABİLECEK ÖNLEMLER

Günümüzde kredi kartı işlemleri, kart verilerinin iletimi ve kart verilerinin güvenliği, Ödeme Kartı Endüstrisi (PCI) ve Veri Güvenlik Standartı (DSS) tarafından sağlanmaktadır. Belirlenen standartlar katmansal açıdan güvenliği pekiştirmek için oluşturulmuş standartlardır. Fakat günümüzde birçok şirket kaynak yetersizliğinden dolayı bu standartları doğru bir şekilde uygulayamamaktadır. Bunun sonucunda da söz konusu şirketler saldırganlar için açık bir hedef haline gelmektedir. Kurumlar RAM kazıma saldırılarına karşı etkili bir savunma sağlamak için ilk olarak, kurum ağı içerisinde yer alan tüm sistemler üzerindeki işletim sistemlerinin son güncel sürümlerine sahip olduklarından emin olunmalıdır. Kullanıcıların söz konusu güncelleştirme işlemlerini unutma ihtimaline karşı, söz konusu güncelleştirmeler otomatize bir şekilde gerçekleştirilmelidir. Ayrıca mümkün olduğunca sistemler üzerinde korsan yazılım kullanımından kaçınılmalı ve lisanslı yazılımlar kullanılmalıdır. Kurumlar ayrıca dış ağdan, ya da sunuculara erişim yetkisi olmayan bir iç ağdan gelebilecek saldırıları engellemek amacıyla güvenlik duvarı kullanmalıdırlar. Kurumlar ayrıca iyi yapılandırılmış bir güvenlik duvarının yanında, beyaz liste mantığı ile çalışan ve sadece uzmanlar tarafından izin verilmiş uygulamaların sistemler üzerinde çalışmasını sağlayan güvenlik uygulamalarını tercih etmelidirler. Böylelikle şirket güvenlik uzmanı tarafından onaylanmış ve beyaz liste kapsamına alınmış uygulamalar dışında hiçbir uygulama ve yazılım, kritik sunucular üzerinde çalıştırılamayacaktır. Kurumlar ayrıca tam kapsamlı bir koruma sağlamak amacıyla, çalıştırılabilir olan exe, swf, pdf gibi uzantılara sahip tüm dosyaları, indirme sonrasında sistemler üzerinde çalıştırmadan, kendi bünyesinde sanal sistemler üzerinde çalıştıran ve analiz eden aktif ağ cihazlarını da tercih etmelidirler. Kart bilgilerinin geçici olarak da olsa tutulduğu sistemlere ait ağ trafiği kayıt altına alınmalı ve düzenli olarak takip edilmelidir. Şirket içinden gerçekleşebilecek saldırılara karşı önlem almak amacıyla PCI-DSS standartları kapsamında, sunuculara sadece güvenilir kişiler tarafından erişilmesi mümkün kılınmalıdır. Ayrıca sisteme erişim yetkisi olan tüm bireyler için olan bilgi güvenliği politikası oluşturulmalıdır [16].

Kredi kartı verilerinin elde edilmesi amacıyla gerçekleştirilen büyük saldırılar sonrasında, söz konusu bilgilerin güvenliğini sağlamak amacıyla Chip-Pin sistemi getirilmiştir. Fakat bu gelişme sonrasında, saldırılar söz konusu kartların zayıf halkası olan manyetik bant sistemi üzerinden gerçekleştirilmeye devam etmiştir. Bu durumun önüne geçmek için firmalar tarafından uygulanması gereken bazı önlemler bulunmaktadır. Chip-Pin sistemini desteklemeyen uygulamalar, dünya genelinde herhangi bir alış-veriş merkezi veya ATM sisteminde kullanılmamalıdır. Kullanılacak cihazlar Chip-Pin uygulamalarını ve getirdiği güvenlik önlemlerini desteklemelidir. Söz konusu kartlar ile ilgili bir sorun oluştuğunda, kart doğrulama işlemi için manyetik bant alanının kullanılmamasına özen gösterilmelidir. Chip-Pin sistemine sahip kartların, yan kanal analizi ve tersine mühendislik saldırılarına karşı güvenilir olduğunun bağımsız

kuruluşlar tarafından sertifikalandırılması gerekmektedir. Türkiye'de kredi kartlarının ürün ve sistem güvenlik değerlendirmeleri için TS ISO/IEC 15408 standartı kullanılmaktadır. ISO/IEC 15408 sertifikası olmayan akıllı kartlar tercih edilmemelidir [17].

VII. SONUÇ

Araştırma raporlarından elde edilen veriler göstermektedir ki, günümüz siber dünyasında veri istismarı amacıyla gerçekleştirilen saldırılarda en büyük orana, PoS sistemlere yönelik RAM kazıma saldırıları sahiptir. Söz konusu saldırıların bu denli yaygın olmasının nedeni; konaklama, sağlık, perakende satış gibi insan hayatının temel ihtiyaçlarını karşılayan birçok sektörde kredi kartlarının kullanılıyor olmasıdır.

Bu çalışmada PoS sistemlere yönelik gerçekleştirilen RAM kazıma saldırılarının metodolojisi incelenmiştir. Söz konusu saldırıları daha iyi analiz edebilmek adına, kredi kartlarına ait verilerin tutulduğu veri grupları incelenmiştir. Ayrıca söz konusu veri gruplarının RAM' den elde edilebilmesi amacıyla saldırganlar tarafından arama ve doğrulama amaçlı kullanılan algoritmalara değinilmiştir. Çalışmada ayrıca, RAM kazıma saldırılarının başlangıç kaynaklarına değinilmiş, söz konusu saldırılarda kullanılan zararlı yazılımların tarihsel gelişimi incelenmiştir. Çalışma, çeşitli istatistiksel veriler ışığında, söz konusu saldırının etkinliğinin analiz edilmesi ile devam etmiş ve bünyesinde PoS sistemler barındıran firmaların alması gereken bir takım önlemlerin sıralanması ile tamamlanmıştır.

Sonraki çalışmalarda temassız akıllı kartların geliştirilmesindeki süreç, güvenlik açıkları, bu kartlara yönelik saldırılar ve bunlara karşı alınabilecek önlemler ele alınacaktır.

KAYNAKLAR

[1] RAM Kazıyıcılar ve Diğer POS Zararlı Yazılımlar, Bağlantı: https://blog.kaspersky.com.tr/ram-kaziyicilar-ve-diger-satis-noktasi-zararli-yazilimlari/872/, Mayıs 2015

[2] Magnetic Stripe Card, Bağlantı: https://en.wikipedia.org/wiki/Magnetic_stripe_card, Haziran 2015

[3] Track Format of Magnetic Stripe Cards (Track 1 and 2), Bağlantı: http://www.acmetech.com/documentation/credit_cards/magstripe_track_format.html, Haziran 2015.

[4] Kredi Kartı Güvenlik Kodu: CVV2/CVC2/CID, Bağlantı: http://www.tuketicifinansman.net/2008/06/cvv2-cvc2-cid-guvenlik-kodu-kredi.html, Haziran 2015

[5] Validating Credit Card Numbers on Your Order Form, Bağlantı: http://www.regular-expressions.info/creditcard.html, Mayıs 2015

[6] Kredi Kartı Doğrulama – Luhn Algoritması, Bağlantı: http://www.yazilimdilleri.net/YazilimMakale-1830-Kredi-Karti-Dogrulama---Luhn-Algoritmasi.aspx, Mayıs 2015

[7] NitlovePOS Malware Uses Phishing Attacks TO Target POS Terminals, Bağlantı: http://www.bsminfo.com/doc/nitlovepos-malware-uses-phishing-attacks-to-target-pos-terminals-0001, Temmuz 2015

[8] POS RAM Scraper Malwares, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-pos-ram-scraper-malware.pdf, Haziran 2015.

[9] CVE and Candidates as of 20150820, Bağlantı: https://cve.mitre.org/data/downloads/allitems.html, Temmuz 2015

[10] Point Of Sale (POS) Malware, Bağlantı: https://www.elevenpaths.com/wp-content/uploads/2015/06/TDS-PoS-Malware-Telefonica-2015-05.pdf, Temmuz 2015

[11] 2015 Data Breach Investigation Report, http://www.verizonenterprise.com/DBIR/2015/, Temmuz 2015

[12] A Look at Point of Sale RAM Scraper Malware and How It Works, Bağlantı: https://nakedsecurity.sophos.com/2013/07/16/a-look-at-point-of-sale-ram-scraper-malware-and-how-it-works/, Mayıs 2015

[13] Markette Korsan Çıktı Gima Yeni Sisteme Geçti, Bağlantı: http://www.hurriyet.com.tr/ekonomi/4494369_p.asp, Mart 2015

[14] RAM Casusluğu, Bağlantı: https://www.mertsarica.com/ram-casuslugu/, Mayıs 2015

[15] In Home Depot Breach, Investigation Focuses on Self-Checkout Lanes, Bağlantı: http://krebsonsecurity.com/tag/target-data-breach/, Mart 2015

[16] PCI-DSS Nedir? , Bağlantı http://www.logsign.net/blog/index.php/pci-dss/ , Haziran 2015

[17] Manyetik Şeritli Kartlar ve CHIP&PIN Uygulaması, Bağlantı: https://www.bilgiguvenligi.gov.tr/donanim-guvenligi/manyetik-seritli-kartlar-ve-chip-pin-uygulamasi-3.html, Temmuz 2015

Doç. Dr. Ecir Uğur Küçüksille- 1976 yılında Isparta'da doğdu. Lisans eğitimini Gazi Üniversitesi Teknik Eğitim Fakültesi Bilgisayar Sistemleri Öğretmenliği Bölümü'nde tamamladı. Yüksek Lisans Eğitimini Süleyman Demirel Üniversitesi Makine Eğitimi Ana Bilim Dalında yaptı. Doktora Eğitimini Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü İşletme/Sayısal Yöntemler Ana Bilim Dalında tamamladı. Halen Süleyman Demirel Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü'nde öğretim üyesi olarak görev yapmaktadır. Bilgisayar, güvenlik ve yapay zeka alanlarında çalışmaları bulunmaktadır.

Bekir Eray Katı- 1992 yılında Karaman' da doğdu. Lisans eğitimini Süleyman Demirel Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümün'nde tamamladı. Halen Süleyman Demirel Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı' nda yüksek lisans eğitimine devam etmektedir. Araştırma konuları arasında, veri tabanı güvenliği ve sızma testleri yer almaktadır.

Mehmet Ali Yalçınkaya- 1990 yılında Isparta' da doğdu. Lisans eğitimini Süleyman Demirel Üniversitesi Teknik Eğitim Fakültesi Bilgisayar Sistemleri Öğretmenliği' nde tamamladı. Yüksek Lisans Eğitimini Süleyman Demirel Üniversitesi Bilgisayar Mühendisliği Ana Bilim Dalında yaptı. Halen Süleyman Demirel Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü' nde araştırma görevlisi olarak görev yapmakla birlikte, Süleyman Demirel Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı' nda doktora eğitimine devam etmektedir. Araştırma konuları arasında, bilgi güvenliği ve sızma testleri yer almaktadır.