Siber Saldırılarda İstismar Kitlerinin Kullanımı Üzerine Bir Analiz ve Savunma Önerileri

E. U. Küçüksille, M. A. Yalçınkaya, O. Uçar

***Özet*— İnternet üzerinde siber saldırganlar tarafından gerçekleştirilen saldırıların büyük bir kısmının, istismar kitleri aracılığı ile gerçekleştirildiği bilinmektedir. İstismar kitleri hedef sistemlere yönelik saldırıları otomatize etmek için oluşturulmuş, içerisinde hedef sistem üzerinde bulunan güvenlik açıklarından yararlanmaya yönelik olarak casus yazılımlar, istismar kodları ve diğer bileşenlerin bir arada bulunduğu bir platformdur. Bu çalışmada, saldırganlar tarafından istismar kitleri aracılığı ile gerçekleştirilen saldırı tipleri incelenerek, kullanıcılara istismar kitlerine karşı alınabilecek önlemler sunulmuştur. Ayrıca istismar kitlerinin kaynakları ve hedef aldıkları uygulamalar, araştırma raporlarından elde edilen istatistiki verilerden faydalanılarak incelenmiştir. Gerçekleştirilen çalışma, istismar kitlerinin neden olduğu zararlı yazılım yüklemeleri, sistem tahribatları ve veri hırsızlıkları gibi bilgi güvenliği alanında karşılaşılan önemli problemlere yönelik çözümler sunmaktadır.**

***Anahtar Kelimeler*— Bilgi Güvenliği, İndirme Tabanlı Saldırılar, İstismar Kitleri, Veri Hırsızlığı**

***Abstract*— A major part of the cyber-attacks that are performed by the hackers are carried out by means of the exploit kits. An exploit kit is a platform that is created automate the attacks against the vulnerabilities located on the target system and includes a combination of exploits, spywares and other components that attempt to exploit these vulnerabilities. In this study, we investigated the attack types which are performed by the cyber attackers through the exploit kits and we present different defense methods to prevent attacks of exploit kits. In addition, the source of the exploit kits and the applications they targeted are examined making use of the statistical data that obtained from research reports. Besides, performed study offers solutions against major problems encountered in the field of information security that caused by the exploit kits such as malware installations, destruction of the systems and data theft.**

***Index Terms*— Data Theft, Drive-by Download Attacks, Exploit Kits, Information Security**

I. GİRİŞ

Günümüzde internet siteleri üzerinden hedef sistemlere yönelik zararlı yazılımların indirilmesi ve çalıştırılmasında önemli bir artış gözlemlenmektedir. Bilgisayar kullanıcılarının internete bağlanması ve dış dünya ile etkileşimde bulunmalarını sağlayan en önemli araçlar internet tarayıcılardır. Birçok internet tarayıcısı günümüzde işletim sistemi kurulumlarında otomatik olarak yüklenmektedir. İnternet tarayıcılılarının oldukça sık kullanılması, onları saldırganların kurbanlarına erişmelerinde en önemli köprülerden biri haline getirmiştir. 2014 yılında yapılan bir araştırmaya göre, internet kaynaklı tehditlerin büyük bir çoğunluğunun, kullanıcıların ziyaret etmiş oldukları zararlı internet siteleri ve kullandıkları internet tarayıcılar ile tarayıcı eklentileri üzerinden gerçekleştirildiği tespit edilmiştir[1]. Kullanıcılarına indirme tabanlı saldırılar sunan istismar kitleri ile internet tarayıcıları üzerinde bulunan güvenlik açıkları hızlı bir şekilde keşfedebilmekte ve bu güvenlik açıklarından yararlanılarak zararlı yazılımlar hedef sistemlere yayılabilmektedir [2]. Ayrıca, tüm bu işlemler otomatize olarak gerçekleştirilmektedir. İstismar kitleri, kullanıcılara yönelik kimlik hırsızlığı ya da internet bankacılığı dolandırıcılığı gibi eylemlerden, bir kurumun güvenlik duvarı arkasındaki bir bilgisayara erişim sağlayarak son derece kritik sistemler üzerinde büyük hasarlara neden olmaya kadar varan birçok farklı saldırı senaryolarında başarılı olabilmektedir.

Siber suç piyasalarında istismar kitleri her geçen gün artan bir ivme ile işlem görmektedir. Dünya çapında ki internet kullanıcılarına yönelik saldırıların yaklaşık üçte ikisinden istismar kitleri sorumludur[3]. İstismar kitleri, şahsi bilgisayar kullanıcılarından, kurumsal ağlar içerisinde bulunan kullanıcılara kadar bütün bilgisayar kullanıcıları için ciddi bir tehdit oluşturmaktadır. Bir istismar kitinin en temel karakteristiklerinden biri, temel seviyede bilgisayar kullanma yeteneğine sahip herkes tarafından kullanılabilecek basitlikte bir kullanıma sahip olmasıdır. Çoğunlukla yeraltı forumlarından temin edilebilen istismar kitleri, kullanıcı dostu bir web ara yüzüne sahip olmaları sayesinde kullanıcılarına, bir bilişim teknolojisi uzmanı ya da güvenlik uzmanı seviyesinde teknik bilgiye sahip olmadan, başarılı saldırılar gerçekleştirmelerine olanak sağlamaktadır. İstismar kitlerinin bir diğer avantajı da kullanıcının, hedefe yönelik saldırı işlemlerinde kullanılacak olan istismar kodlarının nasıl oluşturulduğunun bilmesine gerek olmamasıdır [4].

Uluslararası akademik dünyada istismar kitleri konusunda yapılmış çeşitli çalışmalar mevcuttur fakat ülkemizde henüz istismar kitleri konusunda bir çalışma yapılmamıştır. Bunun nedeni, istismar kiti geliştiricilerinin, piyasaya sürdükleri istismar kitlerinin kaynak kodlarının kopyalanmasına engel

E.U. Küçüksille, Süleyman Demirel Üniversitesi Bilgisayar Mühendisliği Bölümü, Merkez, Isparta, Türkiye; (e-posta: ecirkucuksille@sdu.edu.tr)
M.A. Yalçınkaya, Süleyman Demirel Üniversitesi Bilgisayar Mühendisliği Bölümü, Merkez, Isparta, Türkiye (telefon: +90(246)2111381; e-posta: mehmetyalcinkaya@sdu.edu.tr)
O. Uçar, Bilgi Güvenliği Eğitim ve Danışmanlık Ltd.Şti., Kozyatağı, Kadıköy, İstanbul, Türkiye (e-posta:ozan.ucar@bga.com.tr)

olmak amacı ile ürünlerinde çeşitli şifreleme yöntemleri kullanmalarıdır.

Florian Malecki [2] çalışmasında, istismar kitlerinin şirket ağları üzerinde oluşturabileceği zararlara değinmiştir, kurumsal ağları istismar kitlerine karşı daha güvenli hale getirmek için bir takım önlemler ve tavsiyeler sunmuştur. Allodi ve arkadaşları [3] yeraltı forumlarından elde ettikleri 10 farklı istismar kitini, oluşturdukları MalwareLAB adındaki bir izole ortam içerisinde test etmişlerdir. Çalışmalarında zaman içerisinde farklı sistemler üzerindeki yazılım yapılandırmalarını değiştirerek, bu değişmelere karşı istismar kitlerinin esnekliklerini test etmişlerdir. Yazarlar gerçekleştirdikleri testler sonunda, yazılım güncelleme ve yapılandırmalarına karşı istismar kitlerinin iki farklı role büründüğünü belirtmişlerdir. Bazı istismar kitlerinin yazılım güncellemelerine karşı daha esnek olduklarını fakat bunun yanında daha düşük oranlarda enfeksiyon başarısı sağladıklarını, bazı istismar kitlerinin ise yazılım güncellemelerine karşı çok dirençsiz olduklarını fakat etkili oldukları zaman aralıklarında çok yüksek enfeksiyon oranlarına ulaştıklarını belirtmişlerdir. Kotov ve Massacci [5] çalışmalarında, indirme yolu ile gerçekleşen saldırıların arkasındaki temel araçlar olan 30 farklı istismar kitinin kaynak kodlarının ön analizini paylaşmışlardır. Gerçekleştirilen çalışmalar sonunda istismar kitlerinin karakteristik özellikleri çıkartılmış, istismar kitlerinin ip engelleme ve kod şaşırtma tekniklerini kullandıklarını, kullanıcılarına kitleri kişiselleştirme imkânı sağladıklarını ve gerçekleştirilen saldırıları takip edebilmek için istatistiki veriler sağladıklarını belirlemişlerdir. Moyatama ve arkadaşları [6] çalışmalarında, istismar kitleri gibi zararlı yazılımların temin edilebildiği altı farklı yer altı forumu üzerinde çalışmalar gerçekleştirmişlerdir. Gerçekleştirilen çalışmada forumların sosyal ağ yapısı karakterize edilmiş ve bireylerin bu ortamlarda diğer üyelerin güvenlerini kazanmaları veya kaybetmeleri için ne tür durumların oluşması gerektiğine değinilmiştir. Yazarlar ilgili çalışmanın, yeraltı forumlarının sosyal dinamiklerinin ve e-suç pazarının verimliliğinin inceleneceği daha geniş bir araştırma çalışmasının ilk adımı olduğuna değinmişlerdir.

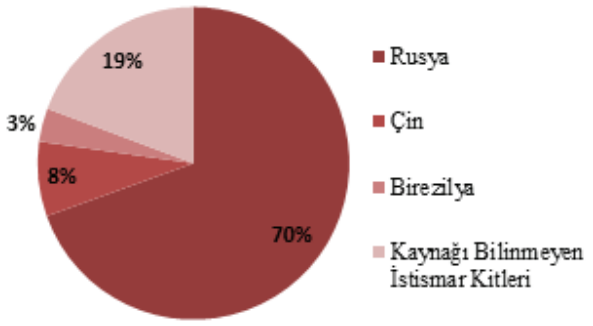
Bu çalışmada; gerçekleştirilmiş diğer çalışmalardan farklı olarak, istismar kitlerinin geliştirildikleri ülkeler, temin edilme süreçleri, kullanıldıkları saldırıların genel akışı ve bu saldırılarda hedef aldıkları uygulamalar çeşitli araştırma raporlarından elde edilen istatistiki veriler ışığında incelenmiş ve istismar kitlerine karşı savunma önerileri sunulmuştur. Çalışmada 2. Bölümde istismar kitleri, üretildikleri ülkeler bazında incelenmiş ve bir istismar kitinin hangi ortamlardan hangi şartlar ile temin edildiği araştırılmıştır. 3. Bölümde istismar kiti tabanlı saldırıların izledikleri genel metodoloji incelenmiş ve saldırılarda hedef alınan uygulamalar istatistiki veriler üzerinde tartışılmıştır. 4. Bölümde, önceki bölümlerde elde edilen verilere dayanarak istismar kitlerine karşı alınabilecek önlemler sunulmuş, 5. Bölümde gerçekleştirilen çalışmanın sonuçlarına değinilmiştir.

II. İSTİSMAR KİTLERİNİN EVRİMİ VE YERALTI PAZARLARDA İSTİSMAR KİTLERİ

Bir istismar kiti, siber suçlular tarafından kullanılan ve indirme tabanlı saldırılar gerçekleştiren yazılım aracıdır. Bir istismar kitinin asıl amacı, hedef sistemler üzerinde yer alan internet tarayıcılarda bulunan güvenlik açıklarından faydalanarak, hedef sistemlere gizlice zararlı yazılım indirmek ve çalıştırmaktır [5]. Siber saldırganların istismar kitlerini kullanarak izledikleri saldırı tekniklerine değinmeden önce, istismar kitlerinin geçmişine ve bir istismar kitinin bir saldırgan tarafından hangi ortamlardan temin edilebileceğine değinmek gerekmektedir.

Üretilen ilk istismar kitleri 2005 yılında piyasaya sürülmüştür. Bugün yayımlanan istismar kitlerinin büyük çoğunluğu, gelişen yer altı siber piyasalarına sahip olan Rusya ve Çin gibi ülkelerde geliştirilmektedir. 2012 yılında yayınlanan bir araştırma raporuna göre, üretilen istismar kitlerinin %69' unun Rusya kaynaklı olduğu belirtilmiştir. Rusya'yı ikinci sırada Çin ve üçüncü sırada da Brezilya' nın izlediği ifade edilmiştir. Araştırmaya mevcut istismar kitlerinin %20' sinin hangi ülke kaynaklı olduğu henüz belirlenememiştir [7]. İstismar kitlerinin üretildikleri ülke oranları Şekil 1' de gösterilmektedir.

Rusya, istismar kitlerini geliştirerek yüksek miktarda kazanç sağlayan siyah şapkalı geliştiriciler ile birlikte uzun bir siber suç geçmişine sahiptir. St. Petersburg merkezli Rusya İş Ağı (RBN) gibi kuruluşlar yıllar boyunca istismar kiti geliştiricilerine bir siber suç platformu sağlayarak istismar kitlerinin gelişmesinde önemli bir rol oynamıştır. RBN yıllar boyunca istismar kiti geliştiricilerine web sitesi hosting imkânı sağlamış, bunun yanı sıra uluslararası alıcılar ile işbirliği yapma ve ürünlerini pazarlamalarına izin vermiştir [4].



Şekil 1. Üretilen istismar kitlerinin ülkelere göre dağılımı[7]

Yasadışı olmanın doğası nedeni ile istismar kitlerinin elde edilmesi zor bir süreçtir. Farklı yetenek ve fonksiyonelliklere sahip istismar kitler yer altı forumlarda farklı fiyat aralıklarında satışa sunulmaktadır [3]. Bu forumlar Google gibi popüler arama motorlarında indekslenmemişlerdir. Bu yüzden söz konusu forumlara erişmek için daha detaylı bir arama işlemi gerçekleştirmek gerekmektedir. Yer altı forumlarına erişim sağlanabilmesi halinde dahi, bir istismar kitinin forumlardan temin edilmesi kolay bir süreç değildir.

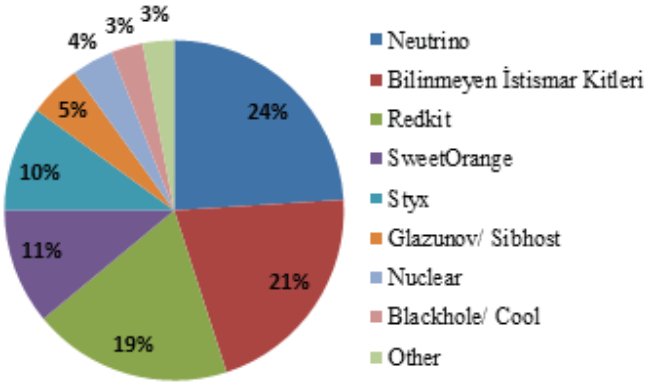
Birçok organize suç grubu gibi, siyah şapkalı siber saldırganlar da kendi özel alanlarına (yeraltı forumları) dışarıdan erişim sağlanmasına kolay kolay izin vermemektedirler. Söz konusu forumların birçoğu için kayıt şartları çok ağırdır ve genellikle kayıt olabilmek için forum içerisinde bir kullanıcıdan referans gerekmektedir. Ayrıca kayıt olma başvurusunda bulunan kişiden, değerlendirme amacıyla geçmiş siber deneyimlerine yönelik bir takım kişisel bilgiler de istenmektedir[4].

Birçok yasal ticari yazılımda olduğu gibi, istismar kitleri de belirli süre aralıklarında tanımlanmış lisanslara sahiptirler. İstismar kitleri için farklı fiyat aralıklarında üç aylık, altı aylık ya da yıllık lisans çeşitleri bulunmaktadır [2]. Kullanıcısına çok fazla fonksiyon olanağı sağlamayan ve bünyesinde, güncelliğini yitirmiş ve yaygın olarak kullanılan istismar kodlarını içeren tipik bir istismar kiti dahi çeşitli fiyat aralıklarında işlem görmektedir. Yeraltı piyasalarında işlem gören en pahalı istismar kitleri ise bünyelerinde çok gizli ve karmaşık istismar kodlarını bulundurmakta, hatta bazı çeşitleri sıfır gün güvenlik açıklarını hedef alan istismar kodlarını içermektedirler. İstismar kiti yazarları, geliştirdikleri ürünler üzerinden maddi kazanç sağladıkları için ürünlerini lisanslamaya önem vermekte, ücretsiz olarak dağıtılmasını ve yayılmasını engellemek için ürünlerinde kaynak kodu koruma, lisanslama, tek bir sunucuya bağlanma gibi teknikler kullanmaktadırlar. Birçok istismar kiti, satıldığı müşterisine ait olan sunucudan farklı bir sunucu altında çalışmasına imkân tanımayan IonCube yazılımı ile korunmaktadır [5].

III. İSTİSMAR KİTİ TABANLI SALDIRILAR VE HEDEF ALDIKLARI UYGULAMALAR

İstismar kitleri, internet tarayıcıları ve tarayıcı eklentileri üzerinde yer alan güvenlik açıklarını hedef alan istismar kodlarını bünyesinde barındıran bir paket olarak tanımlanabilir. İstismar kitleri kurbanlara yönelik indirme tabanlı saldırılar gerçekleştirmektedir. Yapılan çalışmalarda en tehlikeli zararlı yazılım ailelerinin çoğunlukla indirme tabanlı saldırılar ile yayıldıkları tespit edilmiştir [8]. 2013 yılının aralık ayında yayınlanan bir araştırma raporuna göre dünya üzerinde istismar kiti tabanlı saldırılarda kullanılan istismar kitlerinin başında Neutrino istismar kiti gelmektedir. Neutrino istismar kitini ikinci sırada bulunan Redkit istismar kiti izlemektedir. 2012 yılı ve öncesinde Blackhole istismar kiti, dünya genelinde indirme tabanlı saldırılarda en çok kullanılan istismar kiti iken, gerek 2012 yılında piyasaya sürülen yeni istismar kitleri, gerekse geliştiricisinin 2013 yılı ekim ayında tutuklanmasından dolayı, sıralamada yerini kaybetmiştir [9]. 2013 yılında gerçekleşen indirme tabanlı saldırılarda istismar kitlerinin kullanım oranları Şekil 2' de gösterilmiştir.

Bir istismar kiti; işletim sistemi, tarayıcı ya da diğer uygulamaları hedef almak için oluşturulmuş istismar kodlarının bir listesi ile PHP ve HTML dosyalarının bir araya gelmesi sonunda oluşan bir paket olarak tanımlanabilir[8]. Saldırganlar tarafından yeraltı forumlardan temin edilen istismar kitleri, saldırgana ait bir sunucu üzerine bulunan bir web sitesi içerisine yerleştirilmektedirler. Saldırgan çeşitli yöntemler kullanarak kurbanlarının istismar kiti barındıran web sitesini ziyaret etmesini sağlamaktadır. Kurbanın zararlı web sitesini ziyaret etmesi ve istismar kitinin hedef sisteme sızma işleminde başarılı olması durumunda; veri kaybı, fikri mülkiyet hırsızlığı, mali dolandırıcılık ve iş verimliliğinde düşüş gibi sonuçlar ortaya çıkabilmektedir [2].



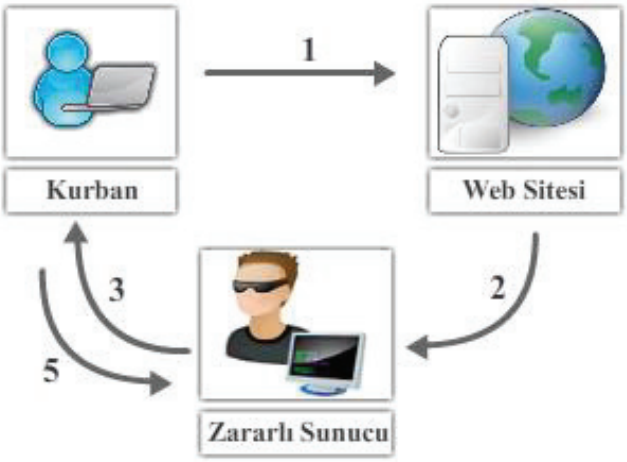
Şekil 2. 2013 yılında siber saldırılarda istismar kitlerinin kullanım oranları [9]

Hedef aldıkları kurbanlarının, istismar kitini bünyesinde barındıran web sitesini ziyaret etmelerini sağlamak için saldırganlar tarafından çeşitli yöntemler kullanılmaktadır. Bu yöntemlerden ilki, kurbanların dikkatlerini çekebilecek mesajlar ya da resimler ile birlikte istismar kitlerinin bulunduğu web sitesine yönlendiren bir web adresini içeren sosyal mühendislik mailleri göndermektir. Fakat günümüzde bilgisayar kullanıcılarının bu tarz maillere karşı nispeten daha bilinçli hale gelmeleri nedeni ile saldırganlar farklı yolları tercih etmektedirler. Saldırganların izlediği bir diğer strateji su kaynağı (watering hole) olarak adlandırılan saldırılardır. Bu tip saldırılarda, saldırganlar hedef aldıkları kullanıcılar ile doğrudan etkileşim kurmak yerine, hedef kullanıcıların ziyaret ettiklerini düşündükleri masum web sitelerini hedef almaktadır. Saldırganlar masum web sitelerini istismar ederek, bu web sitelerini ziyaret eden kullanıcıların istismar kiti barındıran zararlı web sitesine yönlendirilmelerini sağlamaktadırlar [10].

Saldırganlar tarafından yukarıda kullanılan teknikler göz önüne alındığında, istismar kitlerinin kullanıldığı saldırılarda Şekil 3' te gösterilen akış izlenmektedir.

Birinci adımda kurban, siber saldırganlar tarafından içerisine, ziyaretçileri istismar kiti barındıran bir web sunucusuna yönlendiren bir iframe' in enjekte edildiği istismar edilmiş bir web sitesini ziyaret etmektedir. İkinci adımda kurban, aracı sunucular üzerinden istismar kitinin bulunduğu sayfanın sunucusuna yönlendirilmektedir. Üçüncü adımda istismar kiti kurbanın bilgisayarına yönelik bilgi toplama işlemi gerçekleştirmekte ve hedef sistem üzerinde kullanılacak olan istismar kodlarını belirlemektedir. Saldırının dördüncü adımında belirlenen güvenlik açığına yönelik olarak kullanılacak olan istismar kodu temin edilmekte ve hedef sistemine gönderilmektedir. Eğer istismar kodu hedef sistem üzerinde başarılı olursa beşinci adımda saldırganın hedef

sistem üzerinde çeşitli eylemlerde bulunmasına olanak sağlayan özel bir zararlı yazılım, hedef sisteme gizlice indirilmekte ve çalıştırılmaktadır [2,5].

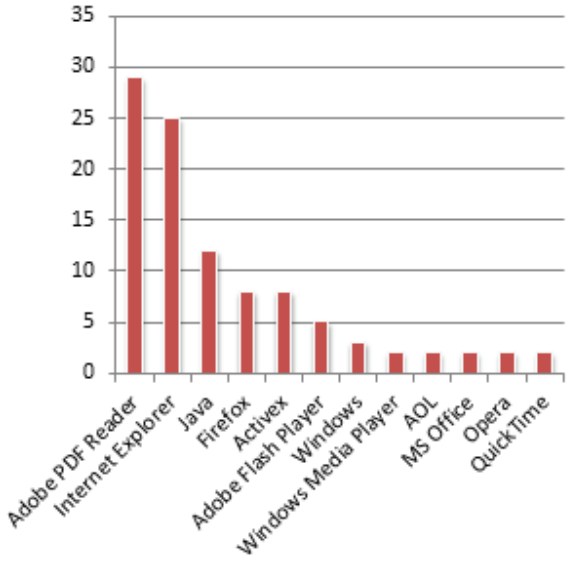


Şekil 3. İstismar kiti tabanlı saldırıların genel akışı

İstismar kitleri çoğunlukla Java, Flash, Adobe Acrobat, Internet Explorer yazılımları ve Windows işletim sistemleri üzerinde bulunan güvenlik açıklarını hedef almaktadır [2]. İstismar kit üreticileri, günümüz bilgisayar kullanıcıları arasında popüler olarak kullanılmakta olan uygulamaların bir listesini oluşturmakta ve bu listeye göre geliştirdikleri istismar kitlerini çeşitli istismar kodları ile donatarak saldırılarda başarı oranlarını arttırmaktadırlar. Örneğin, internetin yaygınlaşması bütün bilgisayar kullanıcıları internet üzerinde işlem yapmak için çeşitli internet tarayıcılarını kullanmaktadırlar. İnternet tarayıcılar ile birlikte gelen çeşitli tarayıcı eklentileri ise saldırganların hedef aralıklarını genişletmektedirler.

2011 yılında KasperskyLAB araştırmacıları tarafından gerçekleştirilen bir araştırmaya göre günümüzde istismar kitlerinin hedef aldıkları uygulamaların %35' ini Internet Explorer, Firefox ve Opera tarayıcıları oluşturmaktadır. Bu da saldırganların hedef aralığında internet tarayıcıların ne kadar önemli bir yer kapladığını göstermektedir. Araştırma verileri incelendiğinde, bilgisayar kullanıcıları arasında popüler olarak kullanılmakta olan Adobe Reader, Oracle Java, Windows Media Player, Adobe Flash, Microsoft Office gibi uygulamalar ise toplam hedef alınan uygulamaların %50' sini oluşturmaktadır [11]. Şekil 4' te istismar kitleri ile gerçekleştirilen saldırılarda hedef alınan uygulamalar ve hedef alınma oranları gösterilmektedir.

İstismar kitleri kullanılarak gerçekleştirilmiş saldırılardan başlıcalarına örnek olarak Hindistan devlet sitelerinden biri olan Küçük ve Orta Ölçekli İşletmeler Bakanlığı web sitesinin 2013 yılının mayıs ayında istismar edilmesi örnek gösterilebilir. Söz konusu web sitesi kullanıcılarını Black Hole istismar kiti barındıran bir sunucuya yönlendirmek üzere istismar edilmiştir[12].



Şekil 4. İstismar kitleri tarafından hedef alınan uygulamalar[11]

2013 yılının ekim ayında ise, günümüzde alexa.com sıralamasına göre dünya üzerinde en çok ziyaret edilen 241. web sitesi olan php.net sitesi, ziyaretçilerini Magnitude adında bir istismar kitini barındıran bir sunucuya yönlendirmek üzere saldırganlar tarafından istismar edilmiştir [13]. İstismar kiti kullanılarak gerçekleştirilen en etkili saldırılardan bir tanesi, 28 Nisan 2014 tarihinde, alexa.com verilerine göre dünya üzerinde en çok ziyaret edilen 89. web sitesi konumunda olan dünyanın en popüler video paylaşım sitelerinden Dailymotion' ın istismar edilmesi ile gerçekleştirilmiştir. Saldırganlar ziyaretçileri, üzerinde Sweet Orange adında bir istismar kiti barındıran bir web sitesine yönlendiren bir iframe'i Dailymotion web sitesine enjekte etmişlerdir. Böylelikle Internet Explorer, Adobe Flash Player ve Oracle Java üzerindeki güvenlik açıklarını hedef alan Sweet Orange istismar kiti, kullanıcıların Bilgisayarlarındaki olası güvenlik açıklarını tespit etmekte ve istismar kodlarını (exploitler) kullanıcıların bırakmaktadır [14]. İstismar kitleri kullanılarak Türkiye' de gerçekleştirilmiş saldırılara örnek olarak 2013 yılında Sağlık Bakanlığı' na ait web sitelerinden birinin istismar edilmesi örnek gösterilebilir. İstismar edilen web sitesi ziyaretçilerini, otomatik olarak istismar kiti barındıran bir sunucuya yönlendirmektedir.

Şekil 5'te sağlık bakanlığına ait istismar edilmiş web sayfasının, malwaredomainlist adresinden elde edilen bilgileri gösterilmektedir.

IV. İSTİSMAR KİTLERİNE KARŞI SAVUNMA ÖNERİLERİ

İstismar kitleri, çeşitli saldırı teknikleri ile kurbanın izni olmadan hedef sistemlere istismar kodları indirilebilmekte ve çalıştırılabilmektedir. Birçok istismar kiti, yıllar önce deşifre olmalarına rağmen hala hedef aldıkları sistemler üzerinde göz ardı edilemeyecek düzeyde başarı oranı yakalamaktadırlar.

Date (UTC)	Domain	IP
2013/06/05_20:17	www.tdms.saglik.gov. [redacted] .htm	[redacted]

Reverse Lookup	Description	Registrant	ASN	
-	compromised sites le ads to exploit kit	Salk Bakanl / netsis tem@saglik.gov.tr	9121	

Şekil 5. Sağlık bakanlığına ait istismar edilmiş bir web sitesine ait bilgiler

Günümüzde istismar kitleri tarafından istismar edilen güvenlik açıklarının %60'ı iki yıldan fazla süredir istismar edilmektedir. İstismar kitlerinin, söz konusu güvenlik açıklarını istismar etmede hala bu denli başarılı olmalarının nedeni bilinçsiz kullanıcıların sistemlerini güncel tutmamalarıdır [4]. İstismar kitlerinden korunmak için, kullanıcı bilgisayarları üzerinde yer alan işletim sistemi, internet tarayıcı gibi istismar kitlerinin hedef aldıkları uygulamaların son güncel sürümlerine sahip olduklarından emin olunmalıdır. Kullanıcıların söz konusu uygulamaları güncellemeyi unutma ihtimaline karşı, uygulamaların güncelleştirmeleri otomatize bir şekilde gerçekleştirilmelidir. Ayrıca mümkün olduğunca sistemler üzerinde korsan yazılım kullanımından kaçınılmalı ve lisanslı yazılımlar kullanılmalıdır. Güvenli bir tarayıcı kullanmak ve yazılımları güncel tutmak, istismar kitlerinin başarılı olduğu güvenlik açıklarının büyük çoğunluğunun kapatılmasını sağlayacak ve istismar kitlerinin etkinliğinde büyük bir azalmaya neden olacaktır. Unutulmamalıdır ki, piyasada bulunan birçok eski istismar kiti, hedef alınan sistemler üzerinde yer alan güncellenmemiş yazılımlar nedeni ile hala etkili bir saldırı aracı durumdadır.

Bir kurum bünyesinde hangi sayıda bilgisayar kullanıcısına sahip olursa olsun, istismar kitlerine karşı alabileceği en etkili önlemlerden biri, bünyesindeki çalışanlarına olası tehlikeler ve saldırılara karşı farkındalık sağlamaktır. Çünkü çalışanlar, siber saldırganlar tarafından gerçekleştirilen saldırılar hakkında bilgi sahibi olmaları durumunda olası bir saldırıyı ve gelebilecek zararlı yazılımları tanıyacak, dolayısı ile bu zararlı yazılımların kurumsal ağ içerisine girmesine neden olabilecek bir eylemde bulunmayacaktır. Bunun sağlanması için kurumların bilgi işlem departmanları, kurum yönetimi ile işbirliğinde olmalı, ağ güvenliği ve çalışanların eğitimi gibi kurum ağını daha güvenli hale getirilecek işlemler beraber planlanmalıdır. Periyodik aralıklarla kurum içerisinde ki çalışanlara bilinçlendirme ve farkındalık eğitimleri sağlanmalıdır. Böylelikle kullanıcılar bilinmeyen kişiler aracılığı ile gelen elektronik postalara tıklamama ve güvenliğinden şüphe duyulan web adreslerine yönlendirici linkleri açmama gibi farkındalıklara sahip olacaktır.

Ayrıca günümüzde birçok işletme varolan güvenlik duvarlarının, onları saldırılardan koruyacağına inanmaktadırlar. Gerçekte ise, eski güvenlik duvarları bugün kuruluşlar için ciddi bir güvenlik riski oluşturmaktadırlar. Birinci nesil güvenlik duvarı teknolojisi bugünün internet suçluları tarafından gönderilen zararlı yazılım içeren ağ paketlerini denetlemek ve olası saldırılardan korumak için yetersiz hale gelmiştir [2]. Bu nedenle; işletim sistemlerinde "beyaz liste" mantığı kapsamında yalnızca belirli uygulamaların çalışmasına olanak sağlayan Bit9 gibi uygulamaların kullanımı ile istismar kitlerinin neden olduğu tehditlerden büyük oranda korunabilmektedir. Ayrıca kurumlar, kullanıcılarını sıfırıncı gün (zero day) güvenlik açıklıklarına karşı etkili bir şekilde koruyabilmek için, sezgisel çalışma ve analiz yeteneklerine sahip olan aktif ağ cihazları kullanmalıdırlar. Bu sistemler, exe, bat, swf, pdf gibi uzantılara sahip olan çalıştırılabilir tüm uygulamaları, kendi içlerinde barındırdıkları sanal sistemler üzerinde davranışsal olarak analiz edebilmekte ve istismar kitlerinin neden olduğu tehditleri tespit edebilmektedirler. Eğer bir kurum, siber saldırılara karşı ciddi tehdit altında ise, istismar kitleri ve diğer çeşitli saldırı türlerine karşı önceden haber alma ve etkili korunma sağlamak amacıyla "siber istihbarat" hizmeti veren çeşitli kurumlar ile ortaklaşa bir çalışma yürütebilmektedirler.

Kurumlar içerisinde kullanılan ağ ve güvenlik cihazlarından çok fazla miktarda log üretilmektedir. Üretilen logların kurum bilgi işlem personelleri tarafından düzenli aralıklarla kontrol ve analiz edilmesi, kurum güvenliği açısından büyük önem taşımaktadır. Bu nedenle kurum içerisinde yer alan tüm sistemlerin log kayıtları merkezi bir sunucuda eş zamanlı olarak toplanmalı ve log kolerasyonu işlemine tabi tutulmalıdır. Bu işlem sonunda elde edilen verilere göre istismar kiti tabanlı saldırılar alarm durumu olarak kaydedilebilmektedir. Böylelikle tanımlanan alarm durumunun gerçekleşmesi anında uygulanmak üzere koruyucu işlemler tanımlanabilmektedir. Çünkü her başarılı ya da başarısız saldırı girişimi mutlaka sistemler üzerinde bir kayıt oluşturmaktadır. Bu kayıtlar uygun kurallar ile kolerasyon işlemine tabi tutularak, saldırı aşamasında ya da başarılı olmuş bir saldırı sonrasında, sistemler üzerinde bıraktıkları izler büyük oranda bulunabilmekte, elde edilen veriler gerekli güvenlik önlemlerinin alınması amacıyla kullanılabilmektedir.

V. SONUÇ

Yapılan araştırmalar göstermektedir ki, istismar kitleri günümüz siber suç dünyasında saldırganlar tarafından kullanılan silahların en başında gelmektedir. İstismar kitlerinin bu denli popüler olmasının başlıca nedenleri; içerisinde düzinelerce istismar kodlarını barındırmak suretiyle saldırganlara çok büyük boyutlarda bir saldırı kütüphanesi sağlaması ve bir sisteme yönelik gerçekleştirilecek sızma denemelerini saldırgandan bağımsız olarak otomatize etmesidir.

Yapılan araştırmalar sonunda sıfır gün istismar kodları da dâhil olmak üzere en güncel istismar kodlarını bünyesinde barındıran istismar kitleri kadar, iki yıldan fazla bir süredir saldırganların kullanımında olan istismar kitleri de saldırılarda başarılı olmaktadırlar. Bunu en temel nedeni ise günümüz bilgisayar kullanıcılarının sistemlerini güncel tutmak konusunda gösterdikleri dikkatsizliktir.

Bu çalışma da istismar kitleri geliştirildikleri ülke bazında incelenmiş, istismar kitlerinin satışa sunulduğu yer altı piyasalarının sosyal karakteristiklerine değinilmiştir. Ayrıca istismar kitleri kullanılarak saldırganlar tarafından gerçekleştirilen saldırı tipleri araştırılmış ve gerçekleştirilen saldırıların genel bir akışı sunulmuştur. Çalışmada istismar kitlerine karşı alınabilecek en temel önlemin kullanıcı bilinçlendirilmesi ve kullanılan sistemlerin güncel tutulması olduğuna değinilmiş ve istismar kitlerine karşı savunma önerileri maddelenmiştir.

KAYNAKLAR

[1] Symantec Corporation. (2014 April). Symantech Internet Security Threat Report 2014 [Online]. Available:http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

[2] F. Malecki, "Defending Your Business From Exploit Kits*", Computer Fraud & Security*, pp. 19-20, 2013.

[3] L. Allodi, V. Kotov and F. Massacci, "MalwareLab: Experimentation with Cybercrime Attack Tools", presented at the 6th Workshop on Cyber Security Experimentation and Test, Berkeley, CA, 2013.

[4] J. Cannell. (2013, February 11). Tools of the Trade: Exploit Kits [Online] Available: http://blog.malwarebytes.org/intelligence/2013/02/tools-of-the-trade-exploit-kits/

[5] V. Kotov, F. Massacci, "Anatomy of Exploit Kits", *Engineering Secure Software and Systems*, Springer Berlin Heidelberg, 2013, pp. 181-196.

[6] M. Motoyama, D. McCoy, K. Levchenko, S. Savage and G. M. Voelker, "An analysis of Underground Forums", in *Proceedings of the ACM Internet Measurement Conference*, Berlin, 2011, pp. 71-80.

[7] Solutionary Incorporated. (2013 January). SERT Quarterly Threat Report- Q4 2012 [Online]. Available: http://www.solutionary.com/_assets/pdf/research/solutionary-sert_q42012_research.pdf

[8] C. Grier, et al., "Manifacturing compromise: the emergence of exploit-as-a-service*",*in *Proceedings of the 2012 ACM Conferance on Computer and Communications Security*, North Carolina,2012, pp. 821-832.

[9] Sophos Limited Company. (2014 January). Sophos Security Threat Report 2014 [Online]. Available: https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf

[10] M. Sarıca, (2013, August 1), İstismar Kiti Nedir [Online], Available: http://www.mertsarica.com/istismar-kiti-nedir/

[11] V. Diaz, M. Preuss. (2011, February 10). Exploit Kits- A Different View [Online]. Available: http://www.securelist.com/en/analysis/204792160/Exploit_Kits_A_Different_View , Şubat 2011

[12] P. Paganini. (2013, May 27). Watering Hole Attacks And Exploit Kits-Indian Gov Site Case [Online], Available: http://securityaffairs.co/wordpress/14725/hacking/watering-hole-attacks-exploit-kits-indian-gov-site-case.html

[13] P. Paganini. (2013, October 26). Php.net Compromised And Redirecting to Magnitude Exploit Kit [Online]. Available: http://securityaffairs.co/wordpress/19070/cyber-crime/php-net-compromised.html

[14] A. Singh. (2014, July 03). Dailymotion Compromised to Send Users to Exploit Kit [Online], Available: http://www.symantec.com/connect/blogs/dailymotion-compromised-send-users-exploit-kit

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.

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

Ozan Uçar- 2006 yılından itibaren profesyonel iş hayatında sızma testleri, Linux sistemlerin güvenliği ve bilişim güvenliği eğitimleri vermektedir. 2010 yılı itibariyle BGA Bilgi Güvenliği Eğitim ve Danışmanlık firmasında bilişim güvenliği üzerine eğitimler vermekte ve sızma test ekibi liderliği yürütmektedir. Çalışma alanları içerisinde sızma testleri, ağ sistemlerinde adli bilişim analizi ve bilişim güvenliği yer almaktadır.