



## ARAŞTIRMA RAPORU

# Lisanssız Yazılımlar ve Siber Güvenlik Tehditleri

Sponsorlar: BSA | Software Alliance

John F. Gantz  
Thomas Vavra  
Victor Lim  
Ocak 2015

Pavel Soper  
Professor Lars Smith (Louisville Üniversitesi)  
Stephen Minton

## GİRİŞ

Bu Araştırma Raporunda, lisanssız yazılımların kullanımı ile kötü amaçlı yazılımla karşılaşma arasındaki ilişki analiz edilmekte ve üç sonuca varılmaktadır; birincisi, iki değişken arasında güçlü bir korelasyon bulunmaktadır; ikincisi, lisanssız yazılım kullanımı kötü amaçlı yazılımlarla karşılaşılacağına güçlü bir *ön göstergesidir* ve üçüncüsü, ampirik neden sonuç bulguları bulunmaktadır.

Analistler, lisanssız yazılımlarla siber güvenlik tehditleri arasında bağlantı olduğunu uzun zamandır biliyor. Örneğin, 2008 ile 2009 yılları arasında "Conficker" solucanı bütün dünyadaki bilgisayarlara yayıldığında, güvenlik analistleri lisanssız yazılım indirmenin bu virüsün bilgisayara bulaşmasının en muhtemel yollarından biri olduğu uyarısında bulunmuştu.<sup>1</sup> Birkaç yıl sonra, 90 ülkede 5 milyon zombi bilgisayar üreten Citadel botnet ağının çökertilmesi sonucunda suçluların, Citadel virüsü taşıyan lisanssız Microsoft Windows sürümlerini satarak virüsün bu bilgisayarın bir kısmına bulaşmasını sağladıkları ortaya çıkmıştı.<sup>2</sup> Bu olayların ardından FBI'nın 2013 yılında lisanssız yazılımların kötü amaçlı yazılımlar içerebileceği yönünde bir tüketici uyarısı yayınlaması şaşırtıcı değildi.<sup>3</sup>

Ancak, lisanssız yazılımla kötü amaçlı yazılımlardan kaynaklanan güvenlik tehditleri arasındaki bağlantının kapsamlı istatistiksel analizi henüz yapılmamıştır. Bu nedenle BSA | Software Alliance, IDC'den bulguları incelemesini istemiştir. Bu analizin bulguları, kamu politikalarının ve yazılımların doğru bir şekilde lisanslanmasını sağlayan şirket düzeyindeki örnek uygulamaların daha güvenli bilişim ortamlarına katkı sağlayacağını güçlü bir şekilde ortaya koymaktadır.

<sup>1</sup> Krebs on Security blogundaki 20 Haziran 2011 tarihli, "Software Cracks: A Great Way to Infect Your PC" başlıklı yazıyı ve ilgili yorumları <http://krebsonsecurity.com/2011/06/software-cracks-a-great-way-to-infect-your-pc/> adresinde okuyabilirsiniz.

<sup>2</sup> Citadel ağının çökertilmesiyle ilgili kısa bir haber BBC News web sitesinde, 6 Haziran 2013 tarihli, "FBI and Microsoft take down \$500m-theft botnet Citadel" başlıklı sayfadan okunabilir. Bkz. <http://www.bbc.com/news/technology-22795074>.

<sup>3</sup> Ağustos 2013'te yayınlanmıştır ve <http://www.fbi.gov/news/stories/2013/august/pirated-software-may-contain-malware> adresinden ulaşılabilir.

## KORELASYONU BELİRLEME

---

Lisanssız yazılımla güvenlik tehditleri arasındaki bağlantıyı ele almak amacıyla IDC, 81 ülkede lisanssız yazılım kullanımı ve siber güvenlik tehdidi oranlarını analiz etmiştir. Bu ülkelerde her iki oranla ilgili güvenilir bilgiler mevcuttur.

Lisanssız yazılım oranları, IDC'nin BSA için iki yılda bir gerçekleştirdiği bir araştırma olan *Küresel Yazılım Araştırması*'ndan<sup>4</sup> alınmış ve siber güvenlik tehdidi bilgileri, aylık 600 milyon kullanıcının bilgisayarlarındaki faaliyete bakan Microsoft'un Güvenlik İstihbarat Raporu'ndan<sup>5</sup> alınmıştır. Bu Araştırma Raporu için kullanılan ölçüt, bir çeyrekte kötü amaçlı yazılım tespit edildiğini rapor eden Microsoft gerçek zamanlı güvenlik yazılımının kullanıldığı bilgisayar yüzdesi olan *karşılaşma oranıydı*. Perspektif açısından dünya genelindeki bilgisayarların yaklaşık %20'sinde 2013 yılında her çeyrekte kötü amaçlı yazılımla karşılaşıldığını rapor etmiştir.<sup>6</sup>

Şekil 1'de lisanssız yazılım kullanım oranı veri noktalarının yanı sıra 2013 yılında 81 ülkenin her biri için hem karşılaştırma oranı hem lisanssız yazılım oranları bulunan kötü amaçlı yazılımla karşılaşma oranı veri noktaları görülmektedir.

---

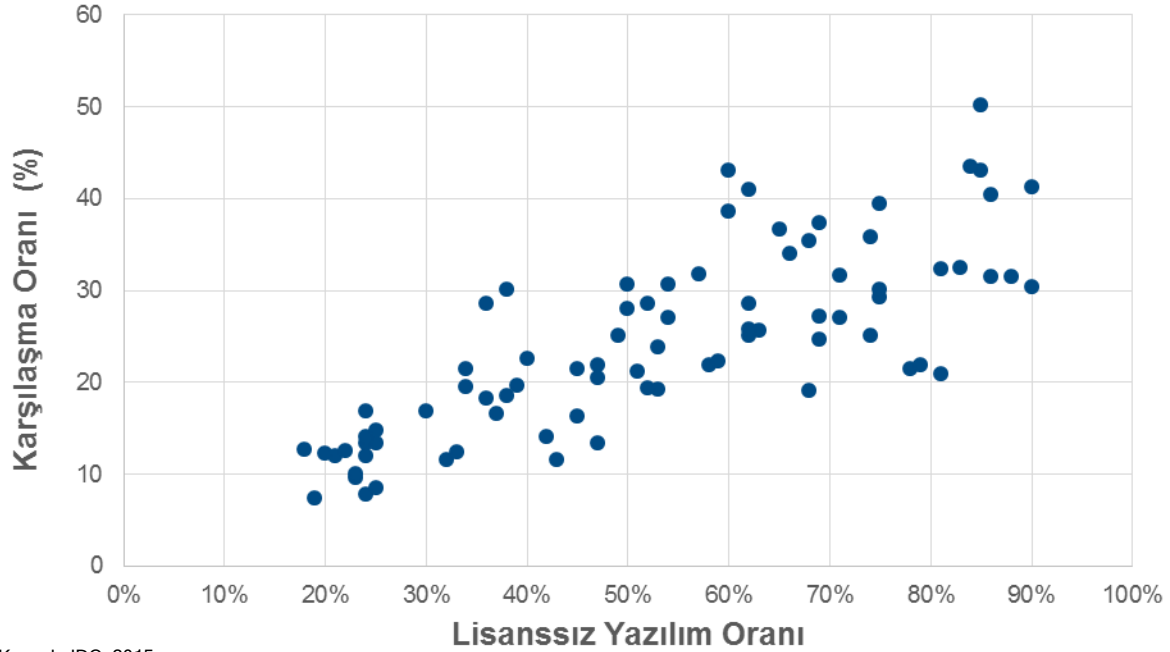
<sup>4</sup> BSA Küresel Yazılım Araştırması: *The Compliance Gap*, Haziran 2014, <http://www.bsa.org/studies> adresinden erişilebilir.

<sup>5</sup> Veri ve metodoloji açıklamaları için <http://www.microsoft.com/security/sir/default.aspx> adresinden ulaşılabilecek Cilt 15 ve 16'ya bakınız.

<sup>6</sup> Siber güvenlik tehditlerini en iyi ölçen araştırma bu mu? Cisco, IBM, Kaspersky, Microsoft, Symantec, Trend Micro ve Verizon gibi şirketlerin yanı sıra hükümet ve bilgisayar acil duruma müdahale ekipleri tarafından yayınlanan başka araştırmalar da var ama bunların çoğu, ülkeye özgü bilgi içerseler bile, hedef konumlara değil tehdit kaynaklarına bakmaktadır. Bilgisayarlar için tasarlanan ve çok sayıda ülkede izlenen bir ölçüt kullanılması, bilgisayar yazılımı kullanımına dayalı bir ölçüte kıyasla da caziptir.

## ŞEKİL 1

### Lisanssız Yazılım Oranları ile Kötü Amaçlı Yazılımla Karşılaşma Oranları Arasında Güçlü Korelasyon Bulunuyor



Her nokta bir ülkenin lisanssız yazılım kullanımının oranını ve kötü amaçlı yazılımla karşılaşma yaygınlığını ifade ediyor. (Verilerin tamamı için Ek'e bakınız.) Model, iki değişken arasında 0,79 gibi istatistiksel olarak güçlü bir korelasyon gösteriyor.

Her iki değer de yukarı yönlü eğilim gösteriyor: bir ülkede lisanssız bilgisayar yazılımı oranı ne kadar yüksekse, bu ülkedeki bilgisayarlarda genellikle daha fazla kötü amaçlı yazılımla karşılaşılıyor.

Örneğin 2013 yılında Amerika Birleşik Devletleri için lisanssız yazılım oranı %18'di ve kötü amaçlı yazılımla karşılaşma oranı her çeyrekte ortalama %13'tü. Endonezya için lisanssız yazılım oranı %84'tü ve kötü amaçlı yazılımla karşılaşma oranı her çeyrekte ortalama %44'tü. Lisanssız yazılım oranı %50 olan Brezilya'da kötü amaçlı yazılımla karşılaşma oranı her çeyrekte %31'di.

İstatistiksel analiz, iki değişken kümesinin güçlü bir pozitif korelasyona sahip olduğunu, yani birlikte yükselip birlikte düştüğünü teyit etmektedir. Bu örnekte korelasyon katsayısı 0,79'dur. 1,0 mükemmel korelasyon olduğunu ve 0 korelasyon olmadığını ifade eder. Karşılaştırma açısından, sigara içme ile

akciğer kanseri arasındaki kolerasyon 0,72'dir,<sup>7</sup> eğitim ile gelir arasındaki korelasyon 0,77'dir<sup>8</sup> ve yolsuzlukla mücadele politikaları ve ekonomik büyüme arasındaki korelasyon 0,77'dir.<sup>9</sup>

Bu korelasyon, neden sonuç ilişkisini ne kanıtlar ne de kanıtlamazken, lisanssız yazılım oranları daha düşük olduğunda, kötü amaçlı yazılımla karşılaşma oranlarının da daha düşük olduğunu açıkça gösteriyor.

## TAHMİN MODELİ OLUŞTURMA

---

Analizde bir sonraki adım, lisanssız yazılım oranlarının kötü amaçlı yazılımla karşılaşmayı *tahmin etmek* için doğru şekilde nasıl kullanılabileceğini göstermek amacıyla bir model geliştirmektir. Yazarlar bu amaçla, bir değişkenin (lisanssız yazılım kullanım oranı) başka bir değişkeni tahmin edebileceği (kötü amaçlı yazılımla karşılaşma oranı) bir formül türetmek için veri kümelerinin kullanımını içeren regresyon analizi adı verilen bir istatistik tekniğinden yararlandı.

Şekil 2'de bu analizin sonuçları görülmektedir. Formül mükemmel çalışırsa, değerlerin tamamı çizgi üzerinde olacaktır. Formül işe yaramazsa, değerler rastgele dağıtılmış olacaktır. Bu durumda değerlerin büyük kısmı çizgiye yakın gruplandı ve 0,62 ile istatistiksel olarak güçlü bir tahmin değeri (R kare olarak bilinir) elde edildi; yani model son derece iyi çalıştı. Bu istatistik, bir ülkenin kötü amaçlı yazılımla karşılaşma oranı ile diğer bir ülkenin karşılaşma oranı arasındaki değişkenliğin %62'sinin, bu ülkelerin ilgili lisanssız yazılım oranlarındaki değişkenliğe bağlanabileceği şekilde yorumlanabilir.

---

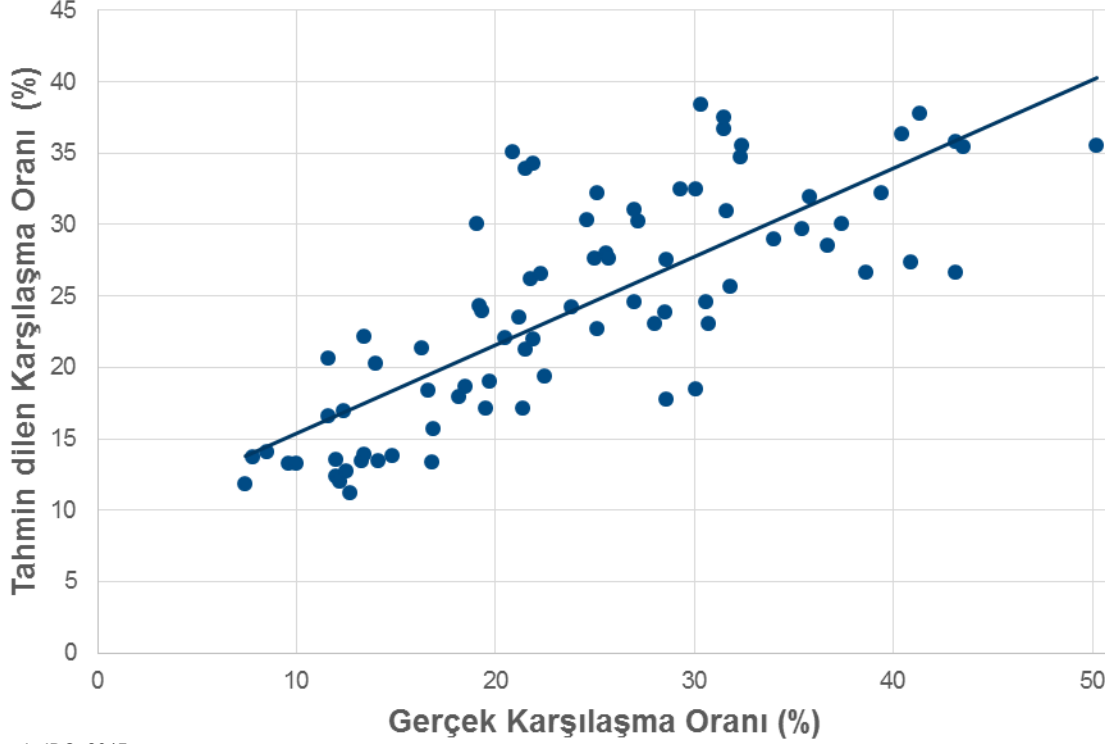
<sup>7</sup> 25 meslek grubunda çalışan binlerce erkek arasında günlük içilen sigara sayısı ile akciğer kanseri oranlarını inceleyen, İngiltere'de gerçekleştirilen bir hükümet araştırmasından alınmıştır. Araştırmanın özetine <http://www3.nd.edu/~busiforc/handouts/Data%20and%20Stories/correlation/smoking%20and%20cancer/smoking.html> adresinden ulaşılabilir ve korelasyon katsayısını elde etmek için kullanılan hesaplamaların ayrıntısına <http://www.spcorexcel.com/correlation-analysis> adresinden ulaşılabilir.

<sup>8</sup> Friedrich Huebler tarafından Ağustos 2008'de hazırlanan, <http://huebler.blogspot.com/2005/09/national-wealth-and-school-enrollment.html> adresinden ulaşılacak International Education Statistics. IDC tarafından Pearson korelasyonu.

<sup>9</sup> "OECD issues paper on corruption and economic growth" başlıklı yazıyı <http://www.oecd.org/g20/topics/anti-corruption/issues-paper-on-corruption-and-economic-growth.htm> adresinde okuyabilirsiniz.

## ŞEKİL 2

### Lisanssız Yazılım Kullanımı, Kötü Amaçlı Yazılımla Karşılaşmanın Güçlü Bir Ön Göstergesidir



Kaynak: IDC, 2015

Her nokta bir ülkenin lisanssız yazılım kullanım oranını ve kötü amaçlı yazılımla karşılaşma oranı tahminini temsil ediyor. (Verilerin tamamı için Ek'e bakınız.) Model, lisanssız yazılım kullanımı ile kötü amaçlı yazılımla karşılaşma arasında 0,62 gibi istatistiksel olarak güçlü bir tahmin değeri (R kare) gösteriyor.

## NEDEN SONUÇ İLİŞKİSİ BULGUSU

Lisanssız yazılım kullanımı ile kötü amaçlı yazılımla karşılaşmanın yüksek korelasyona sahip olması veya regresyon analizinin bir oranın diğerini güçlü bir şekilde tahmin ettiğini göstermesi pek şaşırtıcı gelmeyebilir. Ancak bu bulgular tek başına, lisanssız yazılım oranlarını düşürmenin kötü amaçlı yazılımla karşılaşma oranını düşüreceğini kanıtlamaz. Bu sonuca ulaşmak için istatistiksel analize, neden sonuç ilişkisinin güçlü *ampirik* bulgusu olduğu bağlamında bakılması gerekir.

Bunu bir bağlama oturtmak amacıyla iki değişken çok kolay bir şekilde yüksek korelasyon değerine ama regresyon analizinde düşük bir tahmin değerine sahip olabilir. Bu durum, korelasyon sadece bir tesadüf olduğunda görülür. Örneğin uzun süredir Amerika Birleşik Devletleri'nde dondurma satışları ile cinayet oranları arasında yüksek bir korelasyon olduğu gözlemlenmiştir ancak bunlardan birinin

diğerinin nedeni olmadığı açıktır (ama sıcak hava her ikisinin de nedeni olabilir).<sup>10</sup> Burada ise neden sonuç bulgusu *bulunmaktadır*.

Örneğin, IDC ile Singapur Devlet Üniversitesi (NUS) arasında 2014 yılında yapılan bir araştırma<sup>11</sup>, lisanssız yazılım yüklü olarak satın alınan bilgisayarlarda, lisanssız yazılım DVD'lerinde ve internetten yüklenen lisanssız yazılım ve etkinleştirme anahtarlarında yapılan 800'den fazla testle lisanssız yazılımlarda önemli miktarda kötü amaçlı yazılım olduğunu tespit edilmiştir. Testler, Asya, Avrupa ve Kuzey-Güney Amerika'da bir düzine ülkeyi kapsıyordu. Sonuç: Ortalama olarak bir lisanssız yazılım paketi kullanıcısının kötü amaçlı yazılımla karşılaşma ihtimali üçte birdir.

Dünyadaki lisanssız yazılım paketi sayısı ile bu bulaşma oranının çarpımı, 500 milyondan fazla etkilenen lisanssız yazılım paketinin dolaşımında olduğunu gösteriyor. (Araştırmada, tüketicilerin %40'ından fazlasının otomatik güvenlik güncellemelerini rutin olarak yüklediği tespit edildi. Bu durum da bilgisayarlara kötü amaçlı yazılım bulaşmasına neden olabilir.)

15 ülkeden yaklaşık 1.000 bilgisayarda yapılan benzer bir IDC-NUS araştırmasında, katılımcılardan 5'te 1'i lisanssız yazılımların bilgisayarlarına virüs bulaşmasına neden olduğunu; 5'te 2'si bilgisayarlarını önemli ölçüde yavaşlattığını ve kaldırmak zorunda kaldıklarını (gizli kötü amaçlı yazılımın olası bir işareti) ve 10'da 1'i dosyaları yok ettiğini belirtmiştir.

Bu bulgu göz önünde bulunduğunda, BSA'nın 2013 *Küresel Yazılım Araştırması*'nda bütün dünyadaki bilgisayar kullanıcılarının lisanssız yazılım *kullanmamak* için başlıca neden olarak casus yazılımdan kaynaklanan güvenlik tehditlerini ifade etmiş olmaları şaşırtıcı değildir.

## SONUÇ

---

Bu istatistiksel analiz ve saha bulgusu, lisanssız yazılım ile siber güvenlik tehditleri arasında açık bir bağlantı bulunduğuna işaret etmektedir. Siber güvenlik tehditlerinin tamamı kötü amaçlı yazılımlardan kaynaklanmamaktadır ve kötü amaçlı yazılımların tamamı lisanssız yazılımlardan gelmemektedir. Ama *bazı* kötü amaçlı yazılımların lisanssız yazılımlardan *geldiği* ve kötü amaçlı yazılımların *büyük kısmının* bir siber güvenlik tehdidi oluşturduğu çok açıktır.<sup>12</sup>

---

<sup>10</sup> *Slate*'ten Justin Peters, bu korelasyonla ilgili raporu özetlemiştir. "When Ice Cream Sales Rise, So Do Homicides. Coincidence, or Will Your Next Cone Murder You?" başlıklı, 9 Temmuz 2013 tarihli yazıya [http://www.slate.com/blogs/crime/2013/07/09/warm\\_weather\\_homicide\\_rates\\_when\\_ice\\_cream\\_sales\\_rise\\_homicides\\_rise\\_coincidence.html](http://www.slate.com/blogs/crime/2013/07/09/warm_weather_homicide_rates_when_ice_cream_sales_rise_homicides_rise_coincidence.html) adresinde bakabilirsiniz.

<sup>11</sup> Mart 2014'te yayınlanan *The Link between Pirated Software and Cybersecurity Breaches*. [http://news.microsoft.com/download/presskits/dcu/docs/idc\\_031814.pdf](http://news.microsoft.com/download/presskits/dcu/docs/idc_031814.pdf) adresinde ulaşabilirsiniz. Bu araştırma, lisanssız yazılımlarda karşılaşılan kötü amaçlı yazılımlarla ilgili 2013 ve 2007 yıllarında IDC tarafından yayınlanan önceki araştırmaların ardından yapılmıştır.

<sup>12</sup> 2013 *Veri İhlali Araştırmaları Raporu*'nda Verizon, tehditlerin %40'ının kötü amaçlı yazılımlar içerdiğini ve %71'inin son kullanıcı cihazlarını hedeflediğini ortaya koymuştur. Bkz. [http://www.secretservice.gov/Verizon\\_Data\\_Breach\\_2013.pdf](http://www.secretservice.gov/Verizon_Data_Breach_2013.pdf).

Şirketler, hükümetler ve tüketiciler için açık bir çıkarım, siber güvenlik risklerini azaltmanın bir yolu, lisanssız yazılım kullanımını azaltmaktır. Bunun için etkin yazılım yönetimi politikalarının ve prosedürlerinin uygulanması ve lisanssız yazılımların kullanımıyla ilişkili potansiyel tehlikeler hakkında bilinçlenme sağlamaya kaynak yatırımı yapılması gerekir. Tehlikeler, yazılımın bir parçası olabilen kötü amaçlı yazılımda, kötü amaçlı yazılımın yüklendiği sitelerde ve kaynaklarda ve lisanssız yazılım kullanıcılarının güvenlik güncellemelerini yükleme isteksizliğinde gizlidir. Ama bulgular, lisanssız yazılımın kötü amaçlı yazılımlardan kaynaklanan güvenlik tehditleri ile açıkça ilişkili olduğunu ve bunun küresel maliyetinin, yılda yüz milyarlarca dolara ulaştığını göstermektedir.<sup>13</sup>

---

<sup>13</sup> Bkz. *The Link between Pirated Software and Cybersecurity Breaches*, a.g.e.

## EK – BU ARAŞTIRMADA KULLANILAN ÜLKELER VE VERİLER

Tablo 1 bu araştırmanın kapsadığı ülkelerin ve verilerin bir listesini içermektedir.

**TABLO 1**

### Lisanssız Yazılım Oranı ve Ülkeye Göre Kötü Amaçlı Yazılımla Karşılaşma Oranı, 2013 (%)

Ülke	Lisanssız Yazılım Oranı	Kötü Amaçlı Yazılımla Karşılaşma Oranı
Moldova	90	30
Gürcistan	90	41
Venezuela	88	32
Beyaz Rusya	86	32
Irak	86	40
Cezayir	85	43
Pakistan	85	50
Endonezya	84	44
Ukrayna	83	32
Nijerya	81	21
Vietnam	81	32
Guatemala	79	22
Kenya	78	22
Arnavutluk	75	29
Dominik Cumhuriyeti	75	30
Tunus	75	39
Çin	74	25
Kazakistan	74	36
Lübnan	71	27
Tayland	71	32
Arjantin	69	25
Sırbistan	69	27
Filipinler	69	37



**TABLO 1****Lisanssız Yazılım Oranı ve Ülkeye Göre Kötü Amaçlı Yazılımla Karşılaşma Oranı, 2013 (%)**

Ülke	Lisanssız Yazılım Oranı	Kötü Amaçlı Yazılımla Karşılaşma Oranı
Uruguay	68	19
Ekvador	68	35
Fas	66	34
Peru	65	37
Bulgaristan	63	26
Yunanistan	62	25
Romanya	62	26
Rusya	62	29
Mısır	62	41
Hindistan	60	39
Türkiye	60	43
Şili	59	22
Kuveyt	58	22
Ürdün	57	32
Malezya	54	27
Meksika	54	31
Letonya	53	19
Litvanya	53	24
Hırvatistan	52	19
Kolombiya	52	29
Polonya	51	21
Suudi Arabistan	50	28
Brezilya	50	31
Katar	49	25
Estonya	47	13
Kıbrıs	47	21
İtalya	47	22

**TABLO 1****Lisanssız Yazılım Oranı ve Ülkeye Göre Kötü Amaçlı Yazılımla Karşılaşma Oranı, 2013 (%)**

Ülke	Lisanssız Yazılım Oranı	Kötü Amaçlı Yazılımla Karşılaşma Oranı
Slovenya	45	16
İspanya	45	22
Hong Kong	43	12
Porto Riko	42	14
Portekiz	40	23
Macaristan	39	20
Tayvan	38	19
Kore	38	30
Slovakya	37	17
Fransa	36	18
BAE	36	29
Çek Cumhuriyeti	34	20
Güney Afrika	34	21
İrlanda	33	12
Singapur	32	12
İsrail	30	17
Norveç	25	9
Kanada	25	13
Hollanda	25	15
Finlandiya	24	8
İsviçre	24	12
Almanya	24	13
İngiltere	24	14
Belçika	24	17
İsveç	23	10
Danimarka	23	10
Avusturya	22	13

**TABLO 1**

**Lisanssız Yazılım Oranı ve Ülkeye Göre Kötü Amaçlı Yazılımla Karşılaşma Oranı, 2013 (%)**

Ülke	Lisanssız Yazılım Oranı	Kötü Amaçlı Yazılımla Karşılaşma Oranı
Avustralya	21	12
Yeni Zelanda	20	12
Japonya	19	7
Amerika Birleşik Devletleri	18	13

Kaynak: IDC, 2015

## IDC Hakkında

International Data Corporation (IDC), bilgi teknolojisi, telekomünikasyon ve tüketici teknolojisi pazarlarında piyasa istihbaratı, danışmanlık hizmetleri ve etkinliklerinin lider küresel sağlayıcısıdır. IDC; BT profesyonellerinin, şirket yöneticilerinin ve yatırım topluluğunun teknoloji satın alımları ve iş stratejisinde olguya dayalı kararlar almasına yardımcı olur. 1.100'ün üzerinde IDC analisti, dünya geneli 110'dan fazla ülkede teknoloji ve endüstri fırsatları ve eğilimleri ile ilgili küresel, bölgesel ve yerel uzmanlık sunar. 50 yılı aşkın süredir IDC, müşterilerin önemli iş hedeflerine ulaşmasına yardımcı olmak amacıyla stratejik içgörüler sağlamıştır. IDC, dünyanın lider teknoloji medya, araştırma ve etkinlik şirketi olan IDG'nin bir bağlı ortaklığıdır.

## Global Merkez

5 Speen Street  
Framingham, MA 01701  
ABD  
508.872.8200  
Twitter: @IDC  
idc-insights-community.com  
www.idc.com

---

### Telif Hakkı Bildirimi

IDC Bilgileri ve Verilerinin Dışarıda Yayımlanması – Reklamlar, basın bültenleri veya tanıtım materyallerinde kullanılacak IDC bilgileri için, IDC'nin ilgili Başkan Yardımcısı veya Ülke Müdürü'nden önceden yazılı onay alınmalıdır. Böyle bir taleple birlikte hazırlanan belgenin taslağı da gönderilmelidir. IDC, herhangi bir nedenle bilgilerin dışarıda kullanımına onay vermeme hakkını saklı tutar.

Telif Hakkı 2015 IDC. Yazılı izin alınmaksızın çoğaltılması kesinlikle yasaktır.

