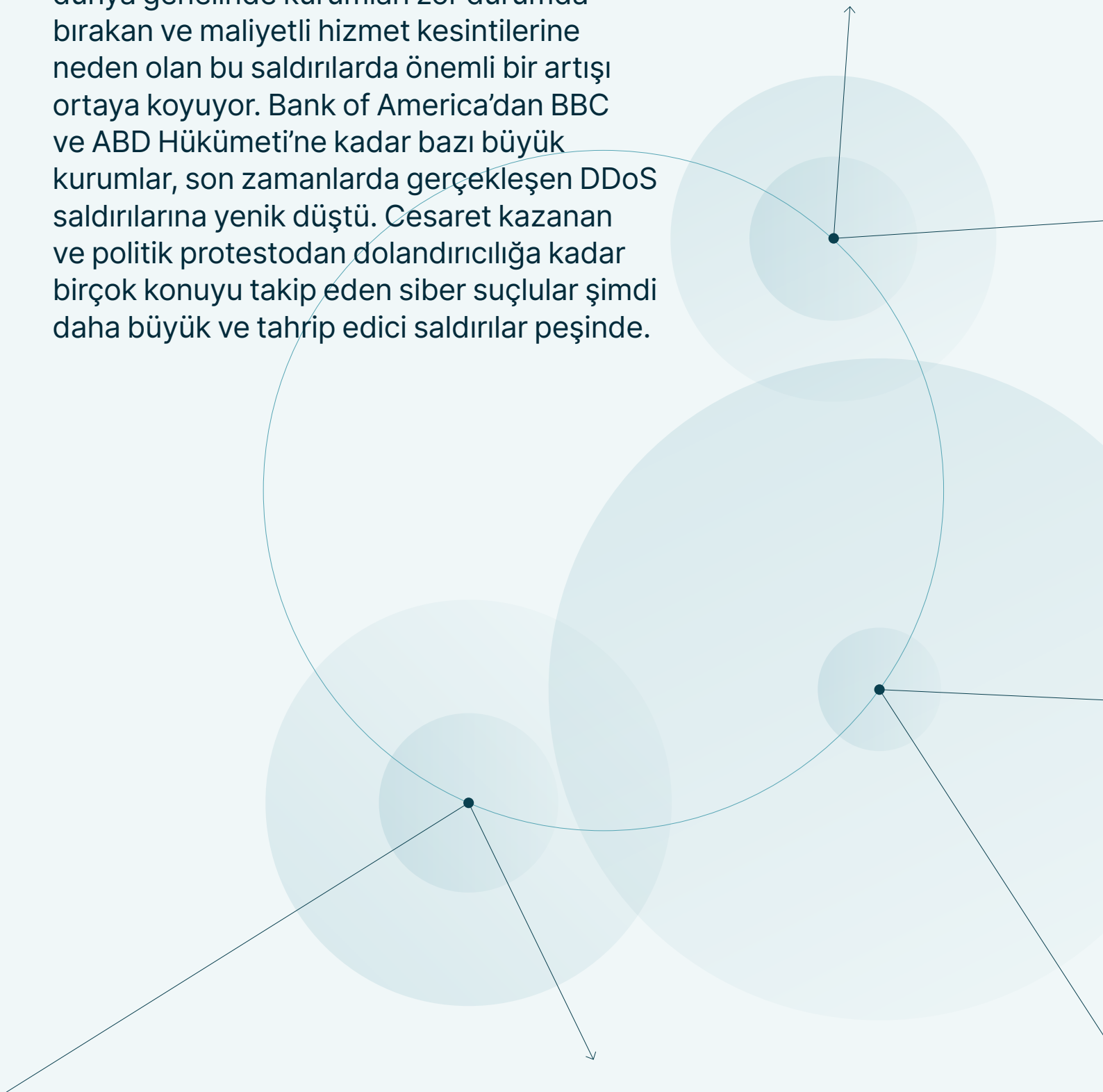
DE-CIX

WHITE PAPER

İnternet Neden Her Zamankinden Daha Fazla Tehdit Altında?

İnternet şüphesiz, hiç olmadığı kadar büyük bir tehdit altında. Güncel raporlar, yıldan yıla yüzde 125 oranında bir artış ile DDoS olarak adlandırılan (Distributed Denial of Service), dünya genelinde kurumları zor durumda bırakan ve maliyetli hizmet kesintilerine neden olan bu saldırılarda önemli bir artışı ortaya koyuyor. Bank of America'dan BBC ve ABD Hükümeti'ne kadar bazı büyük kurumlar, son zamanlarda gerçekleşen DDoS saldırılarına yenik düştü. Cesaret kazanan ve politik protestodan dolandırıcılığa kadar birçok konuyu takip eden siber suçlular şimdi daha büyük ve tahrip edici saldırılar peşinde.



Bir DDoS Saldırısı Nasıl Gerçekleşir?

DDoS saldırıları, yüksek data trafiğine sahip, şüpheli olmayan bir hedefi tetikleyip sisteme yüklenerek çökmesine neden oluyor. Bilgisayar korsanları, yasal olmayan bir şekilde diğer bilgisayar sistemlerine sızıp onları toplu bir saldırı gücüne dönüştürerek bir ağ, servis veya veri tabanını tamamen ele geçirebiliyor. Bu aynı zamanda bir DDoS saldırısının gücünü artırmak için "botnet" kullanma pratiği olarak da ifade ediliyor. Data barajı zayıflarken veya sistemi çökertirken, yasal kullanıcılar erişimlerini kaybediyor. Böylesi saldırılar bir web sitesinin saatlerce hatta günlerce kapalı kalmasına ve kurumların ciddi finansal kayıplar yaşamasına neden olabiliyor.

Neden Bu Saldırılar Büyük Maliyet Yaratıyor?

2014 yılında Incapsula tarafından yapılan bir araştırma, DDoS saldırılarının bir kurum için saatte 40 bin dolara ulaşabilecek bir maliyet oluşturabileceğini öngördü. Saldırıların ortalama 6 ila 8 saat arasında sürdüğü göz önüne alındığında kurumların her saldırıda yarım milyon dolar kaybetmesi söz konusu. Perakende sektörü gibi sektörler için maddi kayıp çok daha katlanarak artabilir. Yitirilen itibar, müşterilerin güvenini kaybetmek ve kritik verilere erişim sağlayamamak ise bu saldırıların diğer önemli sonuçları arasında yer alıyor. Öte yandan, DDoS saldırılarını başlatmak gün geçtikçe kolaylaşıyor. Bazı rakamlar, potansiyel saldırganların kısa sürede büyük bir tahrip yaratmak için saatte yalnızca 10 dolara DDoS servisleri kiralayabileceğini ortaya koyuyor.

Blackholing (Karadelik hizmeti) Nedir?

Karadelik olarak da bilinen blackholing, DDoS saldırılarının etkisini azaltmak için kullanılan bir network teknolojisi. İsminden de anlaşılacağı gibi bu teknoloji, süpheli trafiği network'ten uzaklaştırmak amacıyla bir karadelik

DDoS Nedir?

Distributed denial-of-service (DDoS) saldırı kaynağının birden fazla, hatta çoğu zaman binlerce ve her biri farklı IP adresleri olma durumudur. Bu, alışveriş yapmak ya da bir işi halletmek için giriş kapısında ya da geçitte bekleyen kalabalık bir insan grubunun giriş izinleri olmasına rağmen izin verilmemesine benzetilebilir. Böyle bir durumda normal operasyon sekteye uğrar. DDoS saldırılarının ölçeği, son yıllarda oldukça arttı ve 400Gbit/s'i aştı.

oluşturarak trafiği bloklar. İnternet Servis Sağlayıcıları (ISP'ler) belirli bir IP prefix'ini hedefleyen trafikten kurtulmak amacıyla karadelik teknolojisini kullanır. Bu prefix'in IP adresine doğru yönelen her bir veri erişime kapanır yani "null routed" olur.

İlk Kez Yapılan İnternet Değişim Noktası Blackholing (Karadelik) Çalışması'ndaki Şaşırtıcı Sonuçlar:

Frankfurt'ta bulunan ve dünyanın lider İnternet Değişim Noktası (IXP) olarak faaliyet gösteren, İnternet Değişim Hizmetleri sağlayıcısı DE-CIX, kısa süre önce ilk kez, müşterilerini zararlı DDoS saldırılarından korumak için ISP'lerin blackholing hizmetinden nasıl fayda sağladıklarını gösteren kapsamlı bir araştırma yaptı. Araştırma, ISP'lerin internet trafiği değiş tokuş etmek için bağlandıkları fiziksel altyapıda yani İnternet Değişim Noktası (IXP)'nda bulunan blackholing hizmetine odaklanıyor.

Neden Blackholing (Karadelik)?

İnternet Servis Sağlayıcıları (ISP'ler) belirli bir IP prefix'ini hedefleyen trafikten kurtulmak amacıyla karadelik teknolojisini kullanır. Bu prefix'in IP adresine doğru yönelen her bir veri erişime kapanır yani "null routed" olur, bu veriler "hiçbir yere gitmeyen sanal bir yola" yönlendirilir.

DE-CIX'ten şaşırtıcı sonuçlar:

→ Son 3 aylık dönemde duyurulan 23,000 karadelikle, IXP müşterileri blackholing'i eskiye nazaran daha geniş ölçüde kullanmaya başladı.

→ İncelenen veriler bazında, blackholing'in DDoS saldırılarının etkisini azaltmada ne derece faydalı bir araç olduğu kanıtlandı.

IXP'ler birçok sebepten dolayı, DDoS saldırılarını durdurmada ana noktalardır:

→ Çok sayıda ağın buluşma noktası olması nedeniyle bu tekniğin etkinliği daha da geliştirildi

→ Tek bir route güncellemesi tek seferde tüm müşterilere hitap edebilir

→ İnternetteki merkezi konum göz önüne alındığında, IXP'lerdeki blackholing, saldırı kaynağına daha yakın olanların etkisini hafifletir

→ IXP'lerdeki blackholing, internet üzerindeki rotada bulunan ara ağları koruyabilir ancak etkili olması için saldırı kaynağından yeterince uzaktır.

DE-CIX Neden Blackholing Hizmetini cretsiz Olarak Sunuyor?

DE-CIX, sözkonusu hizmetin İnternet Değişim Noktası (IXP) ekosisteminde sağladığı faydaları da göz önüne alarak müşterilerine blackholing hizmetini ücretsiz olarak sunuyor. Tüm müşterilerinin ağlarını tehdit eden DDoS saldırılarının etkilerini azaltma imkanı veren DE-CIX, artan ağ saldırılarına ve saldırı tekniklerine karşı böylece en iyi savunma hatlarından birini sağlıyor.

Blackholing Neden Kritik Bir Güvenlik Özelliğidir?

DE-CIX, müşterileri tarafından başlatılan bir karadelik hizmeti sunmaktadır. Ağ operatörlerinden biri kendi ağlarından birini hedefleyen bir DDoS saldırısı saptadığında, altyapısını tehdit eden tüm trafiği DE-CIX platformuna yönlendirecek bir routing güncellemesi başlatabilir.

Bu güncelleme, saldırı nedeniyle oluşabilecek yüklemeye karşı operatörün kaynaklarının korunmasını garanti altına alıyor. Karadelik içerisine hapsedilen trafik operatörün portuna asla ulaşamıyor. Bu, yasal internet trafiğini koruyan ve böylece son tüketicilerin servis kesintisi yaşamamasını sağlayan ve gelir kaybının önüne geçen, kritik bir önlem.

DE-CIX'te Blackholing (Karadelik Hizmeti)?

DE-CIX, müşterileri tarafından başlatılan bir karadelik hizmeti sunmaktadır. Ağ operatörlerinden biri kendi ağlarından birini hedefleyen bir DDoS saldırısı saptadığında, altyapısını tehdit eden tüm trafiği DE-CIX platformuna yönlendirecek bir routing güncellemesi başlatabilir.

Kaynakça

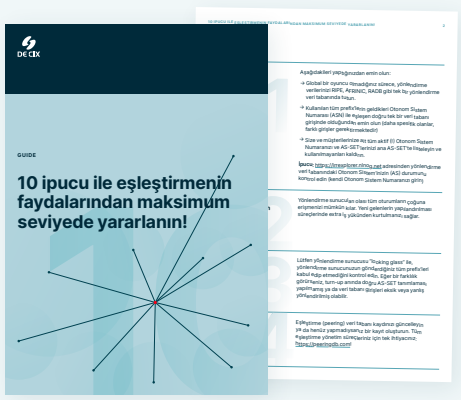
→ www.ahamai.com

→ www.bbc.com

→ www.zdnet.com

→ searchsecurity.techtarget.com

→ www.wired.com



Ek dokümanlar

10 ipucu ile eşleştirmenin faydalarından maksimum seviyede yararlanın
Eşleştirme uzmanı Bernd Spiess, yönlendirme veri tabanı girişlerinden prefix kümelemesine kadar eşleştirme konusunda 10 ipucu hazırladı.

GET IT NOW

DE-CIX Hakkında
Lider İnternet Değişim operatörü ve birbirine bağlantı sağlayıcısı olarak, büyüyen veriyi ve yeni uygulamaları yönetebilmeleri için kurumların yeni fırsatlar ile geleceğe dönük bağlantı ihtiyaçlarını keşfetmelerine katkı sağlıyoruz.
We make interconnection easy. Anywhere.

Daha fazla bilgiye de-cix.net üzerinden ulaşabilirsiniz.

Contact us

Phone: +49 69 1730902-12
Email: sales@de-cix.net