Web Hizmet Dışı Bırakma (DDoS) Saldırılarında Son Dönemdeki Artış ve Korunma Yolları

Arka Plan: Son Saldırı Kampanyalarının Gelişimi

Rusya'nın 24 Şubat 2022'de Ukrayna'yı işgal etmesi yeni bir siber savaş dönemini başlattı. Rusya'nın Ukrayna'ya yönelik siber saldırganlık iddialarına karşılık olarak Ukrayna, Ukrayna Bilişim Ordusu'nu kurarak Rus hedeflerine karşı saldırılar düzenlemek üzere gönüllü Batılı bilgisayar korsanlarını işe aldı. Başlangıçta, siber saldırılar çatışmaya dahil olan iki tarafla sınırlıydı, ancak kısa süre sonra başka hedeflere de yayıldı.

Aralarında NoName057, Killnet kümesi, Anonymous Russia, Passion grubu ve diğerlerinin de bulunduğu Rusya yanlısı bilgisayar korsanı grupları Ukrayna'yı destekleyen ülkelerdeki hedeflere saldırmaya başladı.
Daha yakın zamanda Anonymous Sudan, Mysterious Team Bangladesh ve diğerleri gibi dini gruplar, Müslümanlara hakaret eden hedeflere karşı siber saldırılar başlatarak bu karışıma katıldılar.

Saldırı taktikleri yüksek hacimli ağ tabanlı yoğun akışlı saldırılarla başladı. Daha sonra da tespit edilmesi ve azaltılması zor olan daha karmaşık çok vektörlü uygulama düzeyinde saldırılara dönüştüler.

OpIsrael ve OpsPetir

12 Nisan'da yayınlanan bir uyarıya göre Malezya'da bulunan Filistin yanlısı bir bilgisayar korsan grubu olan DragonForce Malaysia OpsPetir, DragonForce Malaysia İsrail'i hedef alan yeni adlar altındaki operasyonlarına geri döndüğü 3. yılına girdi.

Şekil 1: DragonForce Malaysia OpsPetir

OpIsrael 2023'ün geri dönüşü sırasında ortalıkta görünmeyen tehdit grubu, 11 Nisan'da forumlarında bir basın açıklaması yayınlayarak tüm Müslüman siber savaşçıları, insan hakları savunucularını, gazetecileri ve Malezyalıları İsrail'i hedef alan operasyonlarına katılmaya çağırdı. OpsPetir resmi olarak 12 Nisan'da saat 21:30'da (MYT), İsrail saatiyle 14.30'da başladı ve kurban listesinde büyük bankalar, üniversiteler, hükümet siteleri, İsrail Postası, hastaneler ve diğer önemli hedefler yer alıyor.

Saldırı Yöntemleri

Night Pari olarak da bilinen Pari Malam adlı kullanıcı, OpsPetir için CyberTroopers adlı bir hizmet reddi aracı yayınladı. Karartılmış Python programı, free-proxy-list[.]net ve proxyscrape[.]com adreslerinden internetteki ücretsiz ve açık proxy ve SOCKS hizmetlerinin listelerini indirmek için işlevsellik içerir.

Şekil 2: Cyber Troopers Saldırı Vektörleri ve Proxy Kazıyıcıları Özelliği (kaynak: Radware)

Toplanan proxy ve SOCKS hizmetleri, saldırıların kaynağını taklit etmek ve rastgele hale getirmek ve Katman 7 uygulama saldırıları için tespit ve azaltma karmaşıklığını artırmak için kullanılmaktadır. Grup, aracın TCP, UDP ve HTTP/HTTPS yoğun akış yeteneklerinden yararlanarak, siyasi beyanlarına dikkat çekmek için birçok banka, üniversite, kritik altyapı ve devlet hizmetindeki çevrimiçi hizmetleri ve web sitelerini kesintiye uğratmayı ve geçici olarak devre dışı bırakmayı başardı.

Rusya Yanlısı Bilgisayar Korsanları Karmaşık Teknikler Kullanıyor

Bir yılı aşkın süredir faaliyet gösteren Rusya yanlısı bilgisayar korsanları giderek daha deneyimli ve kullandıkları araçlar da daha karmaşık hale geliyor. NoName057(16) tartışmasız bir şekilde daha karmaşık saldırganlardan birisidir. NoName, her istek için belirli değişkenleri rastgele hale getirirken kurban olarak seçtiği web sitelerine önceden tanımlanmış GET ve POST istekleriyle saldıran gönüllüler tarafından çalıştırılan ve bir ağ üzerinden tekrarlanan görevleri gerçekleştiren otomatik yazılım uygulamaları olan botları dağıtıyor. Saldırı vektörleri bilgileri rastgele hale getirir ancak web sitesi tarafından tanınan meşru argüman ve parametrelerden yararlanır. Meşru talepleri gayrimeşru taleplerden ayırt etmek, saldırganlar tarafından genellikle web içeriğini kullanıcıların bulunduğu yere yaklaştırarak dağıtımını hızlandıran coğrafi olarak dğıtılmış bir grup sunucu olan içerik dağıtım ağlarını (CDN'leri) aşmak için kullanılan rastgele argümanlar eklenmiş saldırı vektörlerini tespit etmeye kıyasla çok daha zordur.

Yeni ve Yıkıcı Web DDoS Saldırıları

Son saldırı kampanyalarında görüldüğü gibi, saldırganlar tek bir kampanyanın parçası olarak birden fazla saldırı türü ve vektöründen yararlanmakta, hem ağ hem de uygulama katmanı saldırı vektörlerini birleştirmekte ve geleneksel yöntemlerle tespit edilmesi ve azaltılması daha zor ve bazen imkansız olan başa çıkılması zor saldırılar oluşturmak için yeni araçlardan yararlanmaktadır.

Saldırganlar bu yeni saldırı araçlarını kullanarak, Web DDoS Tsunami saldırıları olarak da adlandırılan, başa çıkılması daha zor ve daha saldırgan yeni HTTPS akın halindeki saldırı türleri oluşturmaktadır. Bu benzersiz saldırılar, saniye başına düşen çok yüksek isteklerle (RPS) daha yüksek hacimlidir. Şifrelidirler ve meşru talepler gibi görünürler. HTTP yöntemlerini, üstbilgileri ve çerezleri rastgele hale getirmek, popüler gömülü üçüncü taraf hizmetlerini taklit etmek, IP'leri taklit etmek ve diğer önemli hedefler gibi geleneksel uygulama korumalarını atlamak için gelişmiş azaltma tekniklerinden yararlanırlar. Bu son kampanyalarda görülen uygulama düzeyinde saldırı yöntemleri arasında, değişen parametrelerle, proxy'lerin arkasında ve dinamik IP saldırılarıyla HTTPS Get, Push ve Post istek saldırıları vardı. Hepsi de meşru talepler gibi görünüyor.

HTTP/S Akınları ve özellikle Web DDoS Tsunami Saldırılarının azaltılması karmaşıktır.Saldırılar Katman 7'de hareket eder. Bu da saldırı azaltma faaliyetlerinin çoğunun ve özellikle trafiğin incelenmesinin, bağlantı sonlandırıldıktan ve içerik incelendikten sonra yapılması gerektiği anlamına gelir. Trafik proxy'lendikten ve şifrelendikten sonra gerçekleşen saldırı azaltma işlemlerinin tümü, özellikle de ölçekte, nispeten ağır ve onarılması pahalıdır. Bu durum, bu saldırıları potansiyel suçlular için çevrimiçi işletmeleri ve hizmetleri bozmak veya etkilemek için çok cazip bir teknik haline getirmektedir.

Mevcut Korumalar Neden Etkisiz

Şifreli saldırılara geçiş ve bu saldırıların ölçeği ve karmaşıklığındaki artış, tespit için gereken çıtayı yükseltmektedir. Bu değişiklikler, ağ tabanlı DDoS azaltma araçlarının yanı sıra geleneksel şirket içi ve bulut tabanlı, web uygulamalarını siteler arası çeşitli uygulama katmanı saldırılarına karşı koruyan web uygulaması güvenlik duvarı (WAF) çözümlerini bu saldırılara karşı etkisiz hale getirmektedir.
Ağ tabanlı DDoS koruma çözümleri, uygulama katmanı DDoS saldırılarını tespit etmek ve doğru bir şekilde azaltmak için yeterli donanıma sahip değildir. Bu tür saldırıların tespit edilmesi ve azaltılması, saldırı trafiğinin şifresinin çözülmesini ve L7 başlıklarının daha derinlemesine incelenmesini gerektirir. Bu nedenle, bu saldırılar ağ tabanlı DDoS koruma çözümleri tarafından tespit edilememiş olarak kalabilecektir.
İster şirket içi ister bulut tabanlı olsun, standart bir WAF, uygulamaları standart webtabanlı tehditlerden (çoğunlukla OWASP İlk-10) korumak için etkili bir araçtır. Bununla birlikte, aşağıdaki nedenlerden dolayı bu L7 DDoS tehditlerine karşı koruma sağlamada başarısız olmaktadır:

- **Ölçek:** Saniye Başına İstek (RPS) ile ölçülen bu saldırıların bazılarının oranı yeni zirvelere ulaşıyor. Geçtiğimiz yıl, saniyede birkaç milyon istek (RPS) saldırısı çok sayıda üçüncü tarafça gözlemlenmiş ve kamuya açıklanmıştır. Bu oranlar ve trafik hacmi, şirket içi çözümün kapasitesinin çok üzerinde. Buna ek olarak, eğer şirket içi WAF aslında WA File entegre olmuş bir ADC ise, o zaman iş daha da karmaşıktır. Bunun nedeni, ADC'nin saniyede milyonlarca yeni isteği sonlandırmaya ve şifresini çözmeye çalışarak, herhangi bir güvenlik denetimi uygulamaktan bahsetmeksizin azami seviyeye ulaşacak olmasıdır. Sonuç olarak, WAF/ADC'nin kendisi saldırıya maruz kalacak ve yalnızca saldırıya uğrayan URL/alan/uygulama değil, arkasındaki TÜM hizmetler çökecektir. Bu durumda, WAF'a daha fazla kapasite eklemek duruma yardımcı olmayacaktır, çünkü saldırganlar ellerindeki çeşitli yollarla her zaman daha fazla RPS gücü elde edebilirler.

- **Saldırıların Gelişmişliği:** Bu Katman 7 DDoS saldırıları meşru trafik talepleri olarak görünür ve sürekli olarak rastgele ayarlanır (dinamik IP'ler ve diğer parametreler). Aynı şekilde, talepler meşru göründüğü ve belirli bir kötü argüman içermediği için bir bağlantıya dayalı olarak sağlanacak önceden tanımlanmış bir imza veya kural tabanlı bir mekanizma yoktur. Bu nedenle, yalnızca kendi kendine öğrenme ve otomatik ayarlama özelliğine sahip davranışsal tabanlı algoritmalar bu tür saldırıları tespit edebilir ve azaltılabilir.

- **Biçim Değiştiren Saldırılar:** Bu yeni tehditlerin dinamik doğası (vektörleri, kaynak IP'leri ve diğer parametreleri değiştirme ve rastgele hale getirme ve bu değişiklikleri uzun bir süre boyunca sürdürme sıklığı) benzeri görülmemiş bir durumdur. Bu tür saldırılara karşı korunmak için kuruluşların saldırı kampanyasına gerçek zamanlı olarak hızla uyum sağlayabilen çözümlere ihtiyacı vardır. Standart bir şirket içi veya bulut tabanlı WAF bunu sağlayamaz.

- **İnsan Faktörü:** Saldırı kampanyalarının gelişmişliği, saldırıların karmaşıklığıyla başa çıkabilecek ve bir saldırı sırasında koruma kalitesinin tehlikeye atılmamasını sağlayacak güvenlik uzmanlarına sahip olmayı gerektirir. Personel, araç ve bütçe açısından sınırlı olan kendi kendini yöneten ekipler 7x24 devam eden bir saldırı kampanyasıyla başa çıkamaz. Ayrıca, şirket içi araçlar çoğunlukla kural tabanlıdır ve saldırıyı azaltmak için yeni kuralların tanımlanmasını gerektirir. Saldırıyı analiz etmek ve bir kuralı devreye sokmak için gereken süre, saldırının her yinelenmesinde dakikalardan saatlere kadar süren önemli bir kesinti anlamına gelir. Tüm bunlar ve saldırının sürekli bir şekilde değişmesi, sürekli kesinti süresine neden olur.

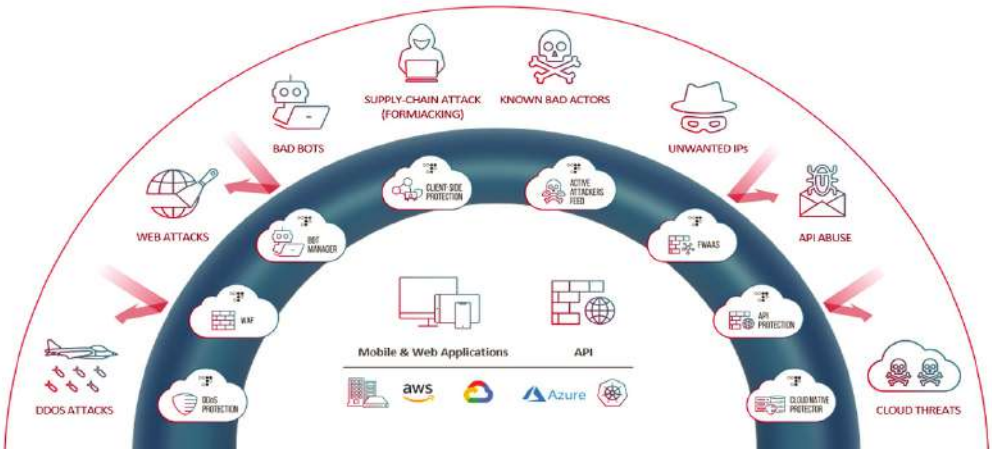
Bunun da ötesinde, geleneksel ek saldırı azaltma yöntemleri bu saldırıları hafifletmede başarılı olamayacaktır. Hız sınırlama tekniklerinden yararlanan çözümler saldırı trafiğini meşru trafikten tam olarak ayırt edemeyecek ve meşru trafiği engelleyecektir. Benzer şekilde, kaynağının coğrafi konumuna göre trafiği engellemek (coğrafi engelleme olarak da bilinir), saldırılar, küresel olarak dağıtılmış ve genellikle hedefin kendisiyle aynı ülkede bulunan botnet'lerden yararlandığı için etkisiz olacaktır.

Korunmak için İhtiyacınız Olanlar

Kapsamlı 360 Derece Bulut Uygulama Koruması
Bu yeni kampanyalara karşı korunmak için kuruluşların kapsamlı, uyarlanabilir bir bulut uygulama koruma hizmetini tercih etmeleri gerekir. Bu hizmet, işletme büyüdükçe ve uygulamalar geliştikçe tehdit vektörlerine karşı korunmalarını sağlarken yönetim yükünü ortadan kaldırır ve en hızlı koruma süresini sağlar.

Radware'in Bulut Uygulama Koruma Hizmeti, tüm uygulama koruma ihtiyaçlarınız için en iyisini, tek noktadan sunar. Türünün en iyisi WAF, bot yönetimi, API koruması, istemci tarafı koruması ve Web DDoS korumasını tek bir çözümde birleştirir. Radware'in Bulut Uygulama Koruma Hizmeti, saldırı altındayken tam olarak yönetilen, kapsamlı koruma sağlamak için Radware'in Acil Durum Müdahale Ekibi (ERT) tarafından desteklenmektedir.

Şekil 3: Radware 360-Derece Bulut Uygulama Koruma Hizmeti



Web DDoS Saldırıları için Yeni Gelişmiş Koruma
Bulut Uygulama Koruma Hizmetinin bir parçası olarak Radware'in yeni Bulut Web DDoS Koruma çözümü, yüksek ölçekli, yeni ortaya çıkan Web DDoS Tsunami saldırılarına karşı ve müşterilere bu tehditlerle mücadele etmek için gereken ölçekte gelişmiş koruma sağlamak için benzersiz bir şekilde tasarlanmıştır. Çözüm şunları sağlar:

1. Saldırıyı Otomatik Olarak Doğru Tespit Etme ve Asgari Yanlış Pozitifli Azaltma

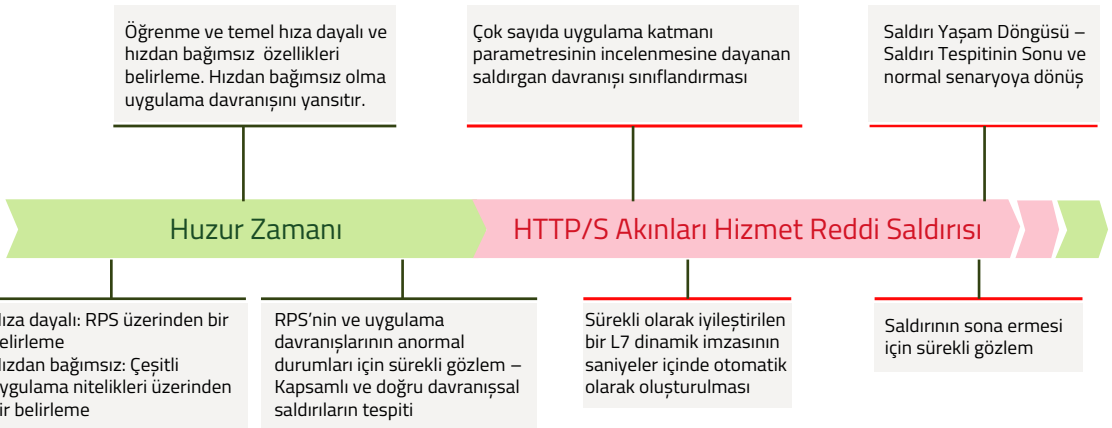
Çözüm, yanlış pozitifleri en aza indirirken ve meşru trafiği engellemezken L7 DDoS saldırılarını hızlı bir şekilde tespit etmek ve cerrahi olarak engellemek için tasarlanmış gelişmiş öğrenme yeteneklerine sahip davranışsal tabanlı algoritmalardan yararlanır. Çoğu tedarikçinin yaygın hacimsel yaklaşımının aksine, Radware'in L7 davranış tabanlı koruması, trafikteki meşru bir artış (diğer adıyla flaş kalabalık) ile düşmanlar tarafından oluşturulan akın halindeki bir saldırıyı doğru bir şekilde ayırt edebilir ve Web DDoS Tsunami saldırıları sırasında bile yalnızca kötü niyetli trafiğin engellenmesini sağlar.

2. En Gelişmiş, Sıfırıncı Gün Saldırılarına Karşı Koruma Sağlayan En Geniş Saldırı Kapsamı

Benzersiz algoritmalar, daha küçük ölçekli, başa çıkılması zor saldırılar, yeni L7 saldırı araçları ve vektörleri ve büyük ölçekli, başa çıkılması zor Web DDoS Tsunami saldırıları dahil olmak üzere çok çeşitli L7 DDoS tehditlerine karşı koruma sağlar. Çözüm, gelişmiş tehditlerin yanı sıra bunların sayısız varyantını da analiz eder ve her türlü saldırı modeline, rastgeleleştirme yöntemine ve saldırı tekniğine (proxy kullanma, meşru botları taklit etme vb.) uyum sağlar.

3. Yüksek Ölçekli Web DDoS Tsunami Saldırıları için En İyi Koruma

Bu yüksek RPS'li (saniye başına istek) başa çıkılması zor L7 DDoS tehditlerine karşı doğru koruma sağlamak için otomatik algoritmaların ve yüksek ölçekli altyapının biraraya gelmesine ihtiyaç vardır.



Şekil 4 : Radware'in Web DDoS Koruması Saldırı Azaltma Yaşam Döngüsü

Çözüm Özeti: Son Web Hizmetdışı Bırakma (DDoS) Tehditleri ve Korunma Yolları

Özet

Web DDoS saldırılarının ölçeği ve gelişmişliği giderek artmaktadır. Son saldırı kampanyalarında gözlemlendiği gibi, saldırı taktikleri yüksek hacimli ağ tabanlı akın halindeki saldırılarla başlamakta ve daha sonra tespit edilmesi ve azaltılması zor olan daha gelişmiş çok vektörlü uygulama düzeyinde saldırılara dönüşmektedir.

Bu yeni tür akın halindeki Web DDoS Tsunami saldırılarını tespit etmek ve azaltmak daha zordur. Bu da onları çevrimiçi işletmeleri ve hizmetleri bozmak veya etkilemek isteyen potansiyel suçlular için son derece çekici teknikler haline getirir. Geleneksel WAF veya ağ tabanlı DDoS koruma çözümleri bu L7 DDoS tehditlerini azaltmakta yetersiz kalmaktadır.

Bu yeni kampanyalara karşı korunmak için kuruluşların, iş büyüdükçe ve uygulamalar geliştikçe tehdit vektörlerine karşı korunmalarını sağlayan, aynı zamanda yönetim yükünü ortadan kaldıran ve en hızlı koruma süresini sağlayan kapsamlı, uyarlanabilir bir bulut uygulama koruma hizmetini tercih etmeleri gerekir.

Radware'in yeni Cloud Web DDoS Koruma çözümü, bu saldırıları engellemek için benzersiz bir şekilde tasarlanmıştır ve meşru trafiği engellemeden L7 DDoS saldırılarını hızlı bir şekilde tespit etmek ve cerrahi olarak engellemek için özel, davranış tabanlı algoritmalardan yararlanır.

- **Kapsamlı Koruma:** Uygulama koruma çözümleri için tek durak noktası: WAF, API koruması, L7 DDoS azaltma ve bot yönetimi.
- **Son Teknoloji Güvenlik:** L3'ten L7'ye kadar tehditler üzerinde uygulanan gelişmiş, patentli, makine öğrenimi tabanlı davranış analizi teknolojisine dayanan bilinen tehditlere ve sıfırıncı gün saldırılarına karşı en geniş kapsama alanı.
- **Azaltılmış Ek Yük:** Otomatik politika oluşturma ile uyarlanabilir koruma ve Radware'in ERT'si aracılığıyla 7x24 devam eden destek.
- **Merkezi Yönetim ve Raporlama:** Nerede konuşlandırılmış olurlarsa olsunlar, uygulamalarınızın güvenliğini yönetmek ve izlemek için tek bir yer.