Derinlemesine Savunma Stratejisi

DDOS

Savunma Stratejileri

El Kitabı

İçindekiler

Genel bakış

Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA), Federal Soruşturma Bürosu (FBI) ve Çok Devletli Bilgi Paylaşımı ve Analiz Merkezi (MS-ISAC), kuruluşlara olasılık ve etkiyi azaltmak için proaktif adımlar sağlamak için bu ortak kılavuzu yayınlıyor. dağıtılmış hizmet reddi (denial-of-service (DDoS))saldırılarının sayısı. Bu saldırılar, bir kuruluşa zaman ve paraya mal olabilir ve kaynaklara ve hizmetlere erişilemezken itibar maliyetleri getirebilir.

DoS ve DDoS

Hizmet reddi (DoS) (Denial-of-service) saldırıları, hedef sistemin kaynaklarını tüketmek amacıyla belirli bir uygulamayı veya web sitesini hedef alan, bu da hedefi ulaşılamaz veya erişilemez hale getiren, _ Meşru kullanıcıların hizmete erişimini engelleyen bir tür siber saldırıdır . Birçok DoS saldırısı türü olmasına rağmen, en yaygın türleri şunlardır:

1. Ağ kaynağının aşırı yüklenmesi, hedefin tüm kullanılabilir ağ donanımını, yazılımını veya bant genişliğini tüketir.
    a. Doğrudan bir ağ kaynağı aşırı yükleme saldırısında, siber tehdit aktörü, bir sunucu güvenlik açığından yararlanmak veya sunucuları isteklerle doldurmak gibi taktikler kullanarak kaynakları aşırı yükler.
    b. Bir yansıma büyütme saldırısında (reflection amplification attack), tehdit aktörü, yüksek hacimli ağ trafiğini hedefe yansıtarak ağ kaynaklarını tüketir. Aktör , verilen sahte kaynak IP adresini barındıran ve yanıtlayan bir aracı olarak üçüncü taraf bir sunucu ("yansıtıcı") kullanır .
2. Protokol kaynağının aşırı yüklenmesi, hedefin kullanılabilir oturumunu veya bağlantı kaynaklarını tüketir.
3. Uygulama kaynağı aşırı yüklemesi, hedefin kullanılabilir işlem veya depolama kaynaklarını tüketir.

DoS saldırısı, aşırı yüklenen trafik, birlikte çalışan birden fazla saldırı makinesinden kaynaklandığında, dağıtılmış hizmet reddi (DDoS) saldırısı olarak sınıflandırılır. DDoS saldırganları, hedeflenen varlığın bakış açısından birçok farklı saldırgandan geliyormuş gibi görünen büyük ölçekli saldırıları gerçekleştirmek için genellikle bir botnet'ten (kaçırılmış internet bağlantılı bir grup cihaz) yararlanır. Nesnelerin İnterneti (IoT) cihazları da dahil olmak üzere çok çeşitli cihazlar bir botnet oluşturabilir. IoT cihazları internete bağlıdır ve genellikle varsayılan şifreleri kullanır ve sağlam güvenlik duruşlarından yoksundur, bu da onları tehlikeye ve istismara karşı savunmasız hale getirir. IoT cihazlarının bulaşması

genellikle kullanıcılar tarafından fark edilmediğinden, bir saldırgan bu cihazlardan yüz binlercesini yüksek hacimli bir saldırı gerçekleştirebilen zorlu bir botnet'te kolayca bir araya getirebilir. Ayrıca, bir siber tehdit aktörü, bir botnet kurduktan sonra, onu vasıfsız kullanıcıların DDoS saldırıları başlatmasını sağlayan bir "kiralık saldırı - attack-for-hire " planıyla diğer potansiyel saldırganlara kiralayabilir.

Bir DDoS saldırısı ne kadar fazla trafik üretirse, bir kuruluşun saldırıya yanıt vermesi ve saldırıdan kurtulması o kadar zor olacaktır. Trafikteki artış, saldırının gerçek kaynağının tespit edilmesini zorlaştırdığından, atıf yapma zorluğunu da artırır. DDoS saldırılarının etkisi genellikle ihmal edilebilir olsa da -saldırının ölçeğine bağlı olarak- ciddi olabilir ve kritik hizmetlerin kaybı veya bozulması, üretkenlik kaybı, kapsamlı iyileştirme maliyetleri ve akut itibar hasarını içerebilir. Kuruluşlar, olaylara müdahale ve operasyonların sürekliliği el kitaplarında bu potansiyel etkileri ele almak için adımlar içermelidir.

Bir DDoS saldırısının bir sistemin ve ilişkili verilerin gizliliğini veya bütünlüğünü etkilemesi pek olası olmasa da, o sistemin meşru kullanımına müdahale ederek kullanılabilirliği etkiler. Siber tehdit aktörü, dikkati gerçekleştirdiği daha kötü niyetli eylemlerden (örneğin, kötü amaçlı yazılım ekleme veya veri sızdırma) uzaklaştırmak için bir DDoS saldırısı kullanabileceğinden, kurbanlar bir DDoS yanıtı boyunca diğer olası güvenlik ihlallerine karşı tetikte kalmalıdır. Mağdurlar, diğer güvenlik izlemelerini görmezden gelecek kadar bir DDoS saldırısına karşı savunmaya odaklanmamalıdır.

Pandemi sonrası ek uzaktan bağlantı gereksinimlerinin olduğu, giderek birbirine bağlı bir dünyada, işletme için temel dış kaynaklı kaynakların kullanılabilirliğini korumak, en olgun BT ve olay müdahale ekipleri için bile zor olabilir. Bir DDoS saldırısının hedefi olmaktan tamamen kaçınmak imkansızdır. Ancak, bir saldırının kaynaklarının kullanılabilirliği üzerindeki etkilerini azaltmak için kuruluşların atabilecekleri proaktif adımlar vardır.

Bir DDoS Saldırısından Önce Hangi Adımları Atmalısınız?

- Kritik varlıklarınızı ve hizmetlerinizi anlayın. Herkese açık internete maruz kaldığınız hizmetleri ve bu hizmetlerin güvenlik açıklarını belirleyin. Varlıklara görev kritikliğine ve kullanılabilirlik ihtiyacına göre öncelik verin. İyi bir siber hijyen taahhüdünde bulunarak saldırı riskini azaltmanın yollarını uygulayın (ör. sunucu güçlendirme, yama). Web uygulaması güvenlik duvarınızın (WAF) kritik varlıklarınızı kapsayıp kapsamadığını ve `_Deny_` durumunda yapılandırılıp yapılandırılmadığını belirleyin.
- Kullanıcılarınızın ağınıza nasıl bağlandığını anlayın. Kullanıcı tabanınızın kuruluşunuzun ağına ister yerinde ister sanal özel ağlar (VPN'ler) aracılığıyla uzaktan

bağlantı kurmasının farklı yollarını belirleyin . Potansiyel ağ geçit noktalarını ve kilit personelin kesintilerini en aza indirebilecek azaltmaları belirleyin.

- Bir DDoS koruma hizmetine kaydolun. Birçok internet servis sağlayıcısının (ISS) DDoS koruması vardır, ancak özel bir DDoS koruma hizmeti, daha büyük veya daha gelişmiş DDoS saldırılarına karşı daha güçlü korumaya sahip olabilir. Sistemleri koruyun ve

  ağ trafiğini izleyebilen, bir saldırının varlığını onaylayabilen, kaynağı tanımlayabilen ve kötü niyetli trafiği ağınızdan uzağa yönlendirerek durumu azaltabilen bir DDoS koruma hizmetine kaydolarak hizmetler. Kuruluşlar, kritik varlık ve hizmetlerin gözden geçirilmesini tamamladıktan sonra bir DDoS koruma hizmetine kaydolmalıdır. Ücretsiz olarak sağlanabilecek hizmetler için CISA'nın Ücretsiz Siber Güvenlik Hizmetleri Kataloğuna bakın .

- Servis sağlayıcı savunmalarını anlayın. Mevcut DDoS korumalarını anlamak için ISS'niz ve bulut hizmeti sağlayıcınızla (CSP) etkileşim kurun. Aşağıdakileri belirlemek için hizmet sözleşmelerini gözden geçirin:
  - hizmet sağlayıcılarınızın DDoS saldırılarını azaltmaya yardımcı olmak için sunduğu korumalar ve
  - Kapsamdaki boşluklar veya sınırlamalardan kaynaklanan herhangi bir risk.

  DDoS korumalarını kullanırken web sunucularını barındırmaya yönelik en iyi uygulamalar hakkında hizmet sağlayıcılarınızla konuşun.

- Özel uç ağ savunmalarınızı anlayın. DDoS saldırılarına karşı koruma sağlayan belirli yönetilen hizmetler hakkında bir yönetilen hizmet sağlayıcısı (MSP) ile konuşun. Uçta farklı teknolojiler sunan MSP'ler, uç savunmalarının özelleştirilmesine yardımcı olabilir. Uç savunma hizmetleri, DDoS saldırılarının neden olduğu kapalı kalma süresini azaltabilir. Uç savunma, algılama ve azaltma hizmetleri, kötü niyetli trafiğin hedefine ulaşma riskini azaltır ve meşru kullanıcıların web sitelerinize/web uygulamalarınıza ulaşma şansını büyük ölçüde artırır.

- Tasarım ve gözden geçirme (Yüksek Kullanılabilirlik/Yük Dengeleme/Kolokasyon) tasarımları. Sistem/ağ tasarımlarını gözden geçirin ve tek bir düğümde barındırılan yüksek değerli varlıklar (HVA) gibi tek hata noktalarını ortadan kaldırın. HVA'ların birden çok düğümde yüksek kullanılabilirlik (HA) ve/veya yük dengeleme (LB) yeteneğine sahip olduğundan emin olun. HVA hizmetlerinin ortak yerleşimi, iş sürekliliği için iyi bir teknik olarak hizmet eder. Ancak, DDoS'a karşı koruma

sağlamanın en iyi yöntemi, yerel veri merkezinizdeki yukarı akış hizmet sağlayıcı savunmaları veya DDoS korumaları tarafından saldırıyı durdurmaktır.

- Bir organizasyon DDoS müdahale planı geliştirin. Müdahale planı, DDoS saldırılarını belirleme, azaltma ve bunlardan hızla kurtulma konusunda kuruluşunuza rehberlik etmelidir. Kuruluşunuzun liderleri ve ağ savunucuları dahil tüm dahili paydaşlar ve hizmet sağlayıcılar, bir DDoS saldırısının tüm aşamalarında rollerini ve sorumluluklarını anlamalıdır. Plan, en azından, bir DDoS saldırısının doğasını anlamayı, bir DDoS saldırısını onaylamayı, azaltmaları dağıtmayı, izlemeyi ve kurtarmayı içermelidir. Not: DDoS müdahale planınız, kuruluşunuzun olağanüstü durum kurtarma planının bir parçası olmalıdır.
- Bir kuruluş DDoS iş sürekliliği planı geliştirin. Planda, özellikle iletişim için kritik uygulamalarınız için alternatifler belirleyin. Özellikle, planın, bir DDoS saldırısının ağınızı bunaltması durumunda, kararları dahili ağ savunucularına veya harici hizmet sağlayıcılara hızlı bir şekilde iletmesi için bir yol içerdiğinden emin olun.
- Bir DDoS saldırısının ağınız için fiziksel yedeklemeleri nasıl etkileyeceğini düşünün. Bir DDoS saldırısının donanımla olan bağlantıları sınırlaması durumunda kuruluşunuzun nasıl çalışabileceğini belirleyin .
- Bir DDoS masaüstü egzersizi yapın ve/veya DDoS yanıt planınızı düzenli olarak test edin. Hizmet sağlayıcılar da dahil olmak üzere tüm iç ve dış paydaşlarla kuruluşunuzun DDoS yanıt planını düzenli olarak uygulamak:
    - Her katılımcının DDoS saldırısı sırasında rollerini ve sorumluluklarını tam olarak anladığından emin olun.
    - Gerçek bir olaydan önce boşlukları ve sorunları belirlemeye yardımcı olun.
    - Paydaşlara, gerçek bir etkinlik sırasında birlikte hareket etmeleri için ihtiyaç duyacakları aciliyet ve ritim duygusu verin.
    - Plana güven oluşturun.

  Her masa üstü alıştırmasından veya testinden sonra bir eylem sonrası incelemesi (AAR) gerçekleştirin ve öğrenilen derslere dayalı olarak DDoS yanıt planını güncelleyin.

Bir Saldırı Yaşadığınızı Düşünüyorsanız Ne Yaparsınız?

- Bir DDoS saldırısının onayı. DDoS saldırılarının süreleri farklıdır. Bir DDoS olayının göstergeleri aşağıdakileri içerebilir, ancak bunlarla sınırlı değildir:

- Dosyaları açarken veya web sitelerine erişirken ağ gecikmesi veya olağan dışı yavaş ağ performansı.
- Yavaş uygulama performansı.
- Yüksek işlemci ve bellek kullanımı.
- Anormal derecede yüksek ağ trafiği.
- Web sitelerinin kullanılamaması veya erişilememesi.

Sizin veya kuruluşunuzun bir DDoS saldırısı yaşadığını düşünüyorsanız, yardım için uygun teknik uzmanlarla iletişime geçmeniz çok önemlidir.

- Kendi uçlarında bir kesinti olup olmadığını veya ağlarının saldırının hedefi olup olmadığını ve sizin dolaylı bir kurban olup olmadığınızı belirlemek için ISS'nize başvurun. Size uygun bir eylem planı hakkında tavsiyede bulunabilirler. Saldırıyı daha iyi anlamak için bulguları servis sağlayıcılara iletin ve onlarla birlikte çalışın.
- Saldırının doğasını anlayın.
  - Saldırıyı yaymak için kullanılan IP adreslerinin aralıkları nelerdir? o Çalışan belirli hizmetlere yönelik belirli bir saldırı olup olmadığına bakın.
  - Sunucu CPU/bellek kullanımını ağ trafiği günlükleri ve uygulama kullanılabilirliği ile ilişkilendirin.
  - Saldırıyı anladıktan sonra, azaltıcı önlemleri devreye alın.
  - DDoS etkinliğinin paket yakalamalarını (PCAP'ler) doğrudan gerçekleştirin veya PCAP'leri elde etmek için güvenlik/ağ sağlayıcılarıyla birlikte çalışın. Güvenlik duvarının kötü niyetli trafiği engellediğini ve meşru trafiğin geçmesine izin verdiğini doğrulamak için PCAP'leri analiz edin.
- Azaltıcıları dağıtın. DDoS saldırılarını engellemek için hizmet sağlayıcılarla çalışmaya devam edin. Mevcut ortamda yapılandırma değişiklikleri yapmayı ve iş sürekliliği planlarını başlatmayı içeren diğer azaltmalar, müdahale ve kurtarmaya yardımcı olabilir. “Test etme ve izleme” sırasında etki azaltma önlemlerini iyice tartışın. Tüm paydaşlar, müdahale ve kurtarmadaki rollerini bilmeli ve anlamalıdır.
- Diğer ağ varlıklarını izleyin. Saldırı sırasında ağınızda bulunan diğer ana bilgisayarları, varlıkları veya hizmetleri gözden kaçırmayın. Tehdit saldırganlarının, dikkatleri hedeflerinden uzaklaştırmak için DDoS saldırıları gerçekleştirdikleri ve bir ağ içindeki diğer hizmetlere ikincil saldırılar gerçekleştirme fırsatını kullandıkları gözlemlendi.

Azaltma ve operasyonel bir duruma geri dönme sırasında saldırıya uğrayan varlıkları izlemeye devam edin. Kurtarma aşamasında, diğer anormalliklere veya uzlaşma göstergelerine dikkat edin. DDoS'un ağınızda devam eden daha kötü niyetli faaliyetlerden yalnızca bir dikkat dağıtıcı olmadığından emin olun.

- DDoS Saldırıları için MS-ISAC Kılavuzunda ana hatlarıyla belirtilen azaltıcı önlemleri kullanın :
    - ISP'nize saldıran IP adresleri sağlayın. Daha fazla trafiği önlemek için kısıtlamalar uygulayabilirler.
        - Yansımalı DDoS saldırılarının genellikle meşru genel sunuculardan kaynaklandığını unutmayın.
        - ISS'nizden bağlantı noktası ve paket boyutu filtrelemesini uygulamasını isteyin.
    - DDoS'un nereden kaynaklanmış olabileceğini belirlemek için kabul edilen ve reddedilen trafiğin güvenlik duvarı günlüğünü etkinleştirin.
    - Kuruluşunuzun başkalarına karşı bir DDoS'ta yansıtıcı olmasını en aza indirmek için, _Deny_ Ağ Zaman Protokolü (NTP) _ `_ monlist _ istek trafiğini (_monlist _ komutunu devre dışı` bırakarak `) tamamen` veya isteklerin geçerli (izin verilen) kaynak adreslerinden gelmesini zorlayın.
    - katı `TCP _keepalive_` ve _ `maksimum_ _bağlantı_` yapılandırmaları tanımlayın.
    - Güvenlik duvarlarını, minimum olarak aşağıdaki IP adreslerinden kaynaklanan gelen trafiği engelleyecek şekilde yapılandırın:
        - _Ayrılmış_ (`0/8`)
        - _Loopback_ (`127.0.0.0/8`)
        - _Özel (RFC 1918 blokları_ `10.0.0.0/8` , `172.16.0.0/12` , ve `192.168.0.0/16`)
        - _Atanmamış DHCP istemcileri_ (`169.254.0.0/16`)
        - TEST-NET-1/2/3 (`192.0.2.0/24` , `198.51.100.0/24` , ve `203.0.113.0/24`)
        - _Çoklu Yayın_ (`224.0.0.0/4`)
        - _Deneysel_ (`240.0.0.0/4`)

Not: Güvenlik duvarı bloklarını yapılandırdıktan sonra, blokların doğru şekilde uygulandığından ve meşru trafiği engellemediğinden emin olmak için ağ trafiğini izleyin.

DDoS Saldırısından Sonra Ne Yaparsınız?

- İkincil bir saldırıya işaret edebilecek herhangi bir ek anormal veya şüpheli etkinlik için diğer ağ varlıklarını izlemeye devam edin.
- Gelecekteki DDoS saldırılarına daha iyi yanıt vermek için DDoS yanıt planınızı güncelleyin. İletişim, azaltma ve kurtarma ile ilgili öğrenilen derslerden çıkarılan iyileştirmeleri dahil edin. DDoS yanıt planınızı düzenli olarak test etmeye devam edin.
- DDoS saldırılarını hızlı bir şekilde belirlemek için ağınızı proaktif olarak izleyin. İzleme, kuruluşunuzun ağ, depolama ve bilgisayar sistemlerinde bir normal etkinlik temeli oluşturmasına olanak tanır. Bu temel, hem ortalama hem de yüksek trafikli günlerdeki etkinliği içermelidir. Bu temelin proaktif ağ izlemede kullanılması, bir DDoS saldırısının erken uyarısını sağlayabilir. Uyarılar, bildirim oluşturacak şekilde yapılandırılabilir, bu da yöneticilerin saldırının başlangıcında yanıt verme tekniklerini başlatmasını sağlar.

Raporlama

CISA ve FBI, DDoS olaylarını derhal yerel bir FBI Saha Ofisine veya CISA'ya report@cisa.gov veya (888) 282-0870 adresinden bildirmenizi tavsiye eder. Eyalet, yerel, kabile ve bölgesel hükümet kuruluşları da MS-ISAC'a (SOC@cisecurity.org veya 866-787-4722) rapor verebilir.

Teşekkür

CISA, FBI ve MS-ISAC, bu danışma belgesine katkılarından dolayı Akamai, Cloudflare ve Google'a teşekkür eder.

sorumluluk reddi

Bu rapordaki bilgiler yalnızca bilgilendirme amacıyla “olduğu gibi” sağlanmaktadır. CISA, FBI ve MS-ISAC, herhangi bir analiz konusu da dahil olmak üzere hiçbir ticari ürünü veya hizmeti onaylamamaktadır. Hizmet markası, ticari marka, üretici veya başka bir şekilde belirli ticari kuruluşlara veya ticari ürünlere, işlemlere veya hizmetlere yapılan herhangi bir referans, CISA, FBI veya MS-ISAC tarafından onay, tavsiye veya kayırma teşkil etmez veya ima etmez.

Kaynaklar

- özel bilgiler için Seçimleri Korumak için CISA'nın Siber Güvenlik Araç Setine bakın .
- Ek DDoS iyileştirme çabaları için MS-ISAC'ın DDoS Saldırıları Kılavuzuna bakın .

- Ek DDoS azaltmaları için bkz. NIST Özel Yayını (NIST SP) - 800-189: Esnek Etki Alanları Arası Trafik Değişimi: BGP Güvenliği ve DDoS Azaltma
- OSI katmanı başına olası saldırı yöntemleri, potansiyel etki, olası DDoS trafik türü açıklamaları ve uygulanabilir önerilen azaltma stratejileri ve ilgili donanım için CISA'nın DDoS Hızlı Kılavuzuna bakın .
- CISA'nın İpucu: Hizmet Reddi Saldırılarını Anlama bölümüne bakın .
- Olayları bozmak için DDoS kullanan siber aktörler hakkında 2022 Pekin Kış Olimpiyatları ve Paralimpik Oyunları Sırasında Olası Siber Faaliyetlere İlişkin FBI Özel Sektör Bildirimine bakın .
- Hacktivizm veya DDoS saldırıları hakkında ek bilgi için, IC3.gov ile ilgili aşağıdaki Kamu Hizmeti Duyurularına bakın .
  - Dağıtılmış Hizmet Reddi Saldırıları Oylama Bilgilerine Erişimi Engelleyebilir,
    Önyükleyici ve Stres Oluşturucu Hizmetlerin Oylanmasını Engellemez
    Dağıtılmış Hizmet Reddi Saldırılarının Ölçeğini ve Sıklığını Artırır
- Aşağıdakiler için Tespit ve Azaltma teknikleri için MITRE ATT&CK'ya bakın:
  - Ağ Hizmet Reddi [T1498] o Doğrudan Ağ Taşması [T1498.001]
    - Yansıma Amplifikasyonu [T1498.002]
- CISA Masa Üstü Egzersiz Paketleri