KASPERSKY DDoS KORUMASI

Kaspersky DDoS Koruması
ile finansal ve tanınırlıkla ilgili
kayıplara karşı işletmenizi korur

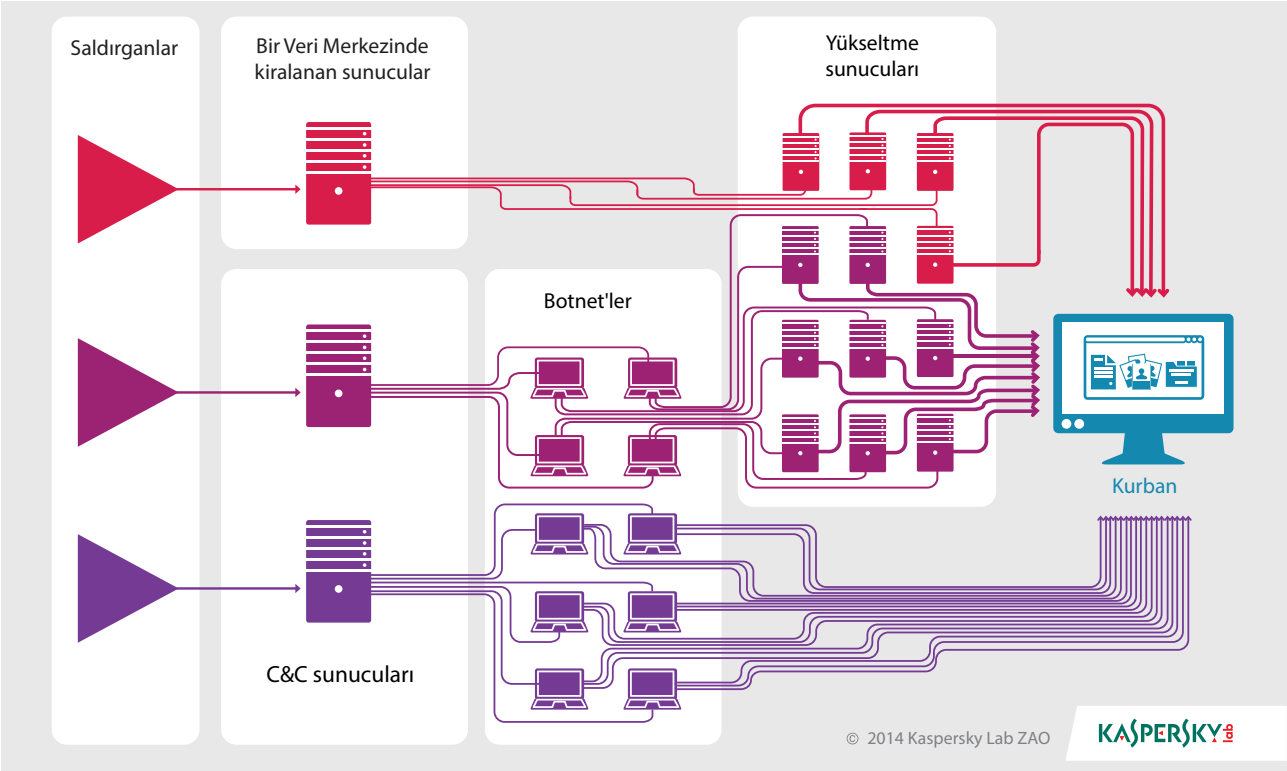
Dağıtılmış Hizmet Reddi (DDoS) saldırısı, siber suçluların cephaneliğindeki en popüler silahlardan biridir. Web siteleri veya veri tabanları gibi bilişim sistemlerine sıradan kullanıcıların normal şekilde erişmesini imkansız hale getirmeyi amaçlar. DDoS saldırılarını başlatmanın arkasında, siber holiganlıktan kirli rekabet uygulamalarına ve hatta gaspa kadar farklı amaçlar olabilir.

Modern DDoS endüstrisi, çok katmanlı bir yapıdır. Saldırıları finanse eden kişiler, kaynaklarını sunan botnet yaratıcıları, saldırıları organize eden ve müşterilerle konuşan aracıları ve sunulan tüm hizmetler için ödemeleri ayarlayan kişileri içerir. Belirli bir sunucu, bir ağ aygıtı veya artık kullanılmayan bir adres gibi İnternette mevcut olan kurban alt ağındaki tüm ağ düğümleri hedef olabilir.

DDoS saldırılarını yürütmek için iki yaygın senaryo vardır: çok sayıda bottan doğrudan saldırıya uğrayan kaynağa istekler gönderme veya yazılım güvenlik açıklarını barındıran, herkes tarafından kullanılabilir sunucular yoluyla DDoS yükseltme saldırısı başlatarak. Birinci senaryoda siber suçlular, çok sayıda bilgisayarı uzaktan kontrol edilen "zombilere" dönüştürür. Bu zombiler de efendilerinin komutuna uyar ve kurban bilgisayar sistemine eş zamanlı olarak istekler gönderir ("dağıtılmış saldırı" yürütür). Bazen DDoS saldırılarını yürütmek ve bir hedefe saldırmaya yönelik emirleri yerine getirmek üzere tasarlanmış özel yazılıma sahip bir grup kullanıcı korsan hacktivistlere yardımcı olur.

Yükseltme saldırısını içeren ikinci senaryoda, botların yerine bir veri merkezinden kiraya verilen sunucular kullanılabilir. Güvenlik açığına sahip yazılımları olan genel sunucular, genellikle geliştirme için kullanılır. Günümüzde DNS (alan adı sistemi) sunucuları veya NTP (ağ süresi protokolü) sunucuları kullanılabilmektedir. Bir saldırı, dönüş IP adreslerini yanıltarak ve daha uzun bir yanıt gerektiren bir sunucuya kısa istek göndererek yükseltilir. Alınan yanıt, kurbana ait olan, yanıltılmış IP adresine gönderilir.

DDoS Saldırı Senaryoları



Şekil 1. En popüler DDoS saldırısı versiyonlarının akış şeması

Durumu çok daha tehlikeli hale getiren başka bir etken daha vardır. Çok sayıda kötü amaçlı yazılım var olduğundan ve siber suçlular çok sayıda botnet oluşturduğundan dolayı neredeyse herkes bu tür bir saldırı başlatabilir. Siber suçlular, herhangi birinin belirli bir siteyi günde 50 dolara yayından kaldırabileceğini söyleyerek hizmetlerinin reklamını yaparlar. Ödemeler genellikle kriptolu dijital para birimiyle yapılır, bu nedenle nakit akışları yoluyla siparişlerin takip edilmesi neredeyse imkansızdır.

Uygun fiyatlar, herhangi bir çevrimiçi kaynağın bir DDoS saldırısında hedef alınabileceği anlamına gelir. Bu yalnızca büyük ve ünlü kuruluşların İnternet kaynaklarıyla sınırlı değildir. Büyük şirketlerin sahip olduğu web kaynaklarına zarar vermek daha zordur, ancak kullanılamaz hale getirildiklerinde bu kesintinin maliyeti çok daha fazla olur. Kaçırılan iş fırsatlarından (elektronik satışlar gibi) kaynaklanan doğrudan kayıpların dışında, şirketler yükümlülüklerini geç yerine getirdikleri için cezalarla ve kendileri daha ileri bir saldırıdan korumalarına yönelik ekstra önlemlerin getirdiği harcamalarla karşılaşabilir. Son ancak önemli bir nokta olarak, şirketin tanınırlığı zarar görebilir; bu da mevcut veya gelecekteki müşterilerin kaybedilmesine yol açabilir.

Toplam maliyet, işletmenin büyüklüğüne, hizmet verdiği sektör segmentine ve saldırı altındaki hizmetin türüne bağlıdır. Analiz şirketi IDC'nin hesaplamalarına göre, bir çevrimiçi hizmetin bir saat boyunca kesintiye uğraması, şirkete 10.000 – 50.000 dolara mal olabilir.

DDoS saldırılarına karşı koyma yöntemleri

Piyasada DDoS saldırılarına karşı korumaya yönelik hizmetler sunan onlarca şirket vardır. Bazıları müşterinin bilişim altyapısına aletler yerleştirirken, bazıları ISS sağlayıcıları dahilindeki kabiliyetleri ve özel temizleme merkezleri yoluyla diğer kanal trafiğini kullanır. Ancak, tüm bu yaklaşımlar aynı prensibi uygular: Önemsiz trafik, yani siber suçlular tarafından yaratılan trafik filtrelenir.

Müşteri tarafında filtreleme ekipmanlarını yerleştirmek, en az etkili yöntem olarak değerlendirilmektedir. Öncelikle, ekipmanın bakımını yapmak ve ekstra maliyetlere neden olan çalışmasını düzenlemek için şirket içinde özel eğitimli personel gerektirir. İkinci olarak, yalnızca hizmet üzerindeki saldırılara karşı etkilidir ve İnternet kanalını tıkayan saldırıları önlemek için hiçbir şey yapmaz. Netten erişilemeyen ama çalışan bir hizmet, hiçbir işe yaramaz. Yükseltilmiş DDoS saldırıları popüler hale geldiğinden, bir bağlantı kanalına aşırı yüklenilmesi çok daha kolaylaştı.

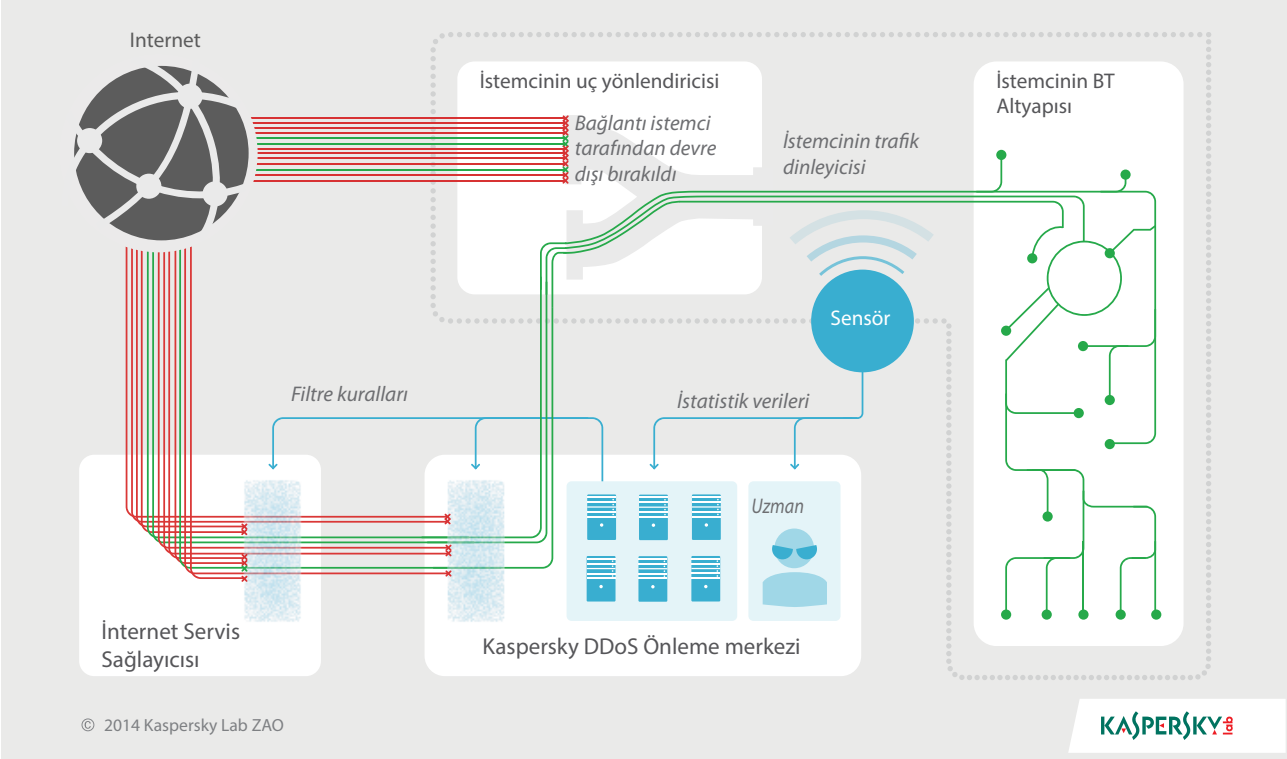
Daha geniş bir İnternet kanalı olduğundan ve tıkanması çok daha zor olduğundan, sağlayıcının trafiği filtrelemesi daha güvenilir bir çözümdür. Diğer yandan, sağlayıcılar güvenlik hizmetleri konusunda uzmanlaşmaz ve yalnızca en belirgin önemsiz trafiği filtreler ve daha küçük saldırıları görmezden gelir. Dikkatli bir saldırı analizi ve anında yanıt, uygun uzmanlığı ve deneyimi gerektirir. Ayrıca, bu tür koruma müşterinin belirli bir sağlayıcıya bağımlı olmasına neden olur ve müşterinin bir yedek veri kanalı kullanması ya da sağlayıcısını değiştirmesi gerektiğinde zorluklar yaratır.

Bu nedenle, çeşitli trafik filtreleme yöntemlerinin bir kombinasyonunu uygulayan uzman işlemenin, DDoS saldırılarını nötr hale getirmenin en etkili yolu olduğu göz önünde bulundurulmalıdır.

Kaspersky DDoS Koruması

Kaspersky DDoS Koruması, veri temizleme merkezlerinin dağıtılmış bir altyapısını kullanarak tüm DDoS saldırısı türlerine karşı koruma sağlayan bir çözümdür. Bu çözüm, sağlayıcı tarafında trafik filtrelemesi, müşterinin altyapısının yanında trafiği analiz etmek üzere uzaktan kontrol edilen bir aletin kurulumu ve esnek filtrelere sahip, uzman temizlik merkezlerinin kullanımını içeren farklı yöntemleri birleştirir. Ayrıca, çözümün çalışması sürekli olarak Kaspersky Lab uzmanları tarafından izlenir, böylece herhangi bir saldırının başlangıcı mümkün olan en kısa sürede algılanabilir ve filtreler gerekli şekilde değiştirilebilir.

Etkin Mod'da Kaspersky DDoS Koruması



Şekil 2. Kaspersky DDoS Koruması: Çalışma Şeması

Kaspersky Lab'in cephaneliği

On yıldan uzun bir süredir, Kaspersky Lab çok çeşitli çevrimiçi tehditlerle başarıyla başa çıkıyor. Bu süre boyunca Kaspersky Lab'in analistleri, DDoS saldırılarının nasıl çalıştığını ayrıntılarıyla öğrenerek benzersiz bir düzeyde uzmanlık kazandı. Şirketin uzmanları, İnternet'te meydana gelen en yeni gelişmeleri sürekli olarak izliyor, siber saldırıları yürütmeye yönelik en son yöntemleri analiz ediyor ve mevcut koruma araçlarımızı geliştiriyorlar. Bu uzmanlık sayesinde, bir DDoS saldırısının başlatılır başlatılmaz ve hedef web kaynağına ulaşmadan hemen önce algılanması mümkündür.

Kaspersky'nin DDoS Koruması teknolojisinin ikinci öğesi, müşterinin BT altyapısının yanına kurulan bir sensördür. Bu sensör, Ubuntu işletim sistemi altında çalışan ve standart x86 sunucusu gerektiren bir yazılım parçasıdır. Kullanılan protokollerin türlerini, gönderilen bit ve veri paketlerinin sayısını, müşterinin web sitesindeki davranışını, yani meta verileri veya gönderilen verilerle ilgili bilgileri analiz eder. Trafiği başka bir yere yönlendirmez, trafiği değiştirir ve tüm mesajların içeriklerini analiz eder. Ardından, istatistikler bulut tabanlı Kaspersky DDoS Koruması altyapısına gönderilir ve burada toplanan meta veriler baz alınarak her müşteri için istatistik tabanlı bir profil oluşturulur. Aslında bu profiller, her müşterinin tipik bilgi alışverişi özelliklerinin kayıtlarıdır. Tipik kullanım sürelerindeki değişiklikler kaydedilir. Daha sonra trafik analiz edilir; trafik davranışının istatistik tabanlı profilden farklı olduğu her durum, bir saldırının göstergesi olabilir.

Kaspersky DDoS Korumasının temeli, temizleme merkezleridir. Bu merkezler ana İnternet omurga hatlarında, Frankfurt ve Amsterdam gibi yerlerde bulunur. Kaspersky Lab eş zamanlı olarak birkaç temizleme merkezini kullanır; böylece, temizlenmesi gereken trafiği bölebilir veya yönlendirebilir. İşleme merkezleri, tek ortak bulut tabanlı bilişim altyapısında birleştirilir ve veriler bu sınırlar olmaksızın saklanır. Örneğin, Avrupalı müşterilerin web trafiği, Avrupa bölgesinden ayrılmaz.

DDoS trafiğini kontrol etmenin başka bir temel yolu, bunu sağlayıcı tarafında filtrelemektir. ISS, sadece bir İnternet kanalı sunmakla kalmaz, aynı zamanda Kaspersky Lab ile teknoloji ortaklığına da girebilir. Bu nedenle, Kaspersky DDoS Koruması, DDoS saldırılarının çoğunda kullanılan en belirgin önemsiz trafiği mümkün olduğunca orijinal noktasına yakın şekilde keser. Böylece, birleşerek tek güçlü saldırı haline gelen akışlar önlenir ve daha karmaşık önemsiz trafiği halletme konusunda serbest olan temizlik merkezleri üzerindeki yük azaltılır.

Trafik yönlendirme araçları

Güvenlik çözümünün etkili şekilde çalışması için ilk temel gereksinim, temizlik merkezleri ve müşterinin BT altyapısı arasında bir bağlantı kanalı oluşturmaktır. Kaspersky DDoS Korumasında bu kanallar, Genel Yönlendirme Kapsüllemesi protokolüne göre düzenlenir. Temizlik merkezi ve müşterinin ağ ekipmanı arasında sanal bir tünel oluşturmak için kullanılır. Temizlenen trafik, bu tünel yoluyla müşteriye iletilir.

Gerçek trafiğin yönlendirilmesi, şu iki yöntemden birini kullanarak yapılabilir: Bir BGP dinamik yönlendirme protokolü kullanarak müşterinin alt ağını duyurarak ya da temizlik merkezinin URL'sini tanıtarak DNS kaydını değiştirerek. İlk yöntem trafiği çok daha hızlı şekilde yönlendirebildiği ve doğrudan belirli bir IP adresini hedefleyen saldırılara karşı koruma sağladığından tercih edilebilir. Ancak, bu yöntem müşterinin bölgesel İnternet memuru tarafından sağlanan IP adreslerinin engellenmesi gibi sağlayıcıdan bağımsız bir adres aralığına sahip olmasını gerektirir.

Söz konusu gerçek yönlendirme prosedürü olduğunda, bu iki yöntem arasında çok küçük bir fark vardır. İlk yöntem kullanıldığı takdirde, müşteri tarafındaki ve temizlik merkezindeki BGP yönlendiricileri, sanal tünel yoluyla kalıcı bir bağlantı kurar; saldırı durumunda ise temizlik merkezinden müşteriye doğru yeni bir rota oluşturulur. İkinci yöntem kullanıldığında, temizlik merkezinin adres havuzundan müşteriye bir IP adresi atanır. Bir saldırı başlarsa müşteri, DNS A kaydındaki IP adresini temizlik merkezi tarafından atanan IP adresiyle değiştirir. Sonrasında müşterinin adresine gelen tüm trafik, önce temizlik merkezine gönderilir. Ancak, eski IP adresi üzerinde süren saldırıyı durdurmak için sağlayıcının temizlik merkezinden gelen veriler dışındaki tüm gelen trafiği engellemesi gerekir.

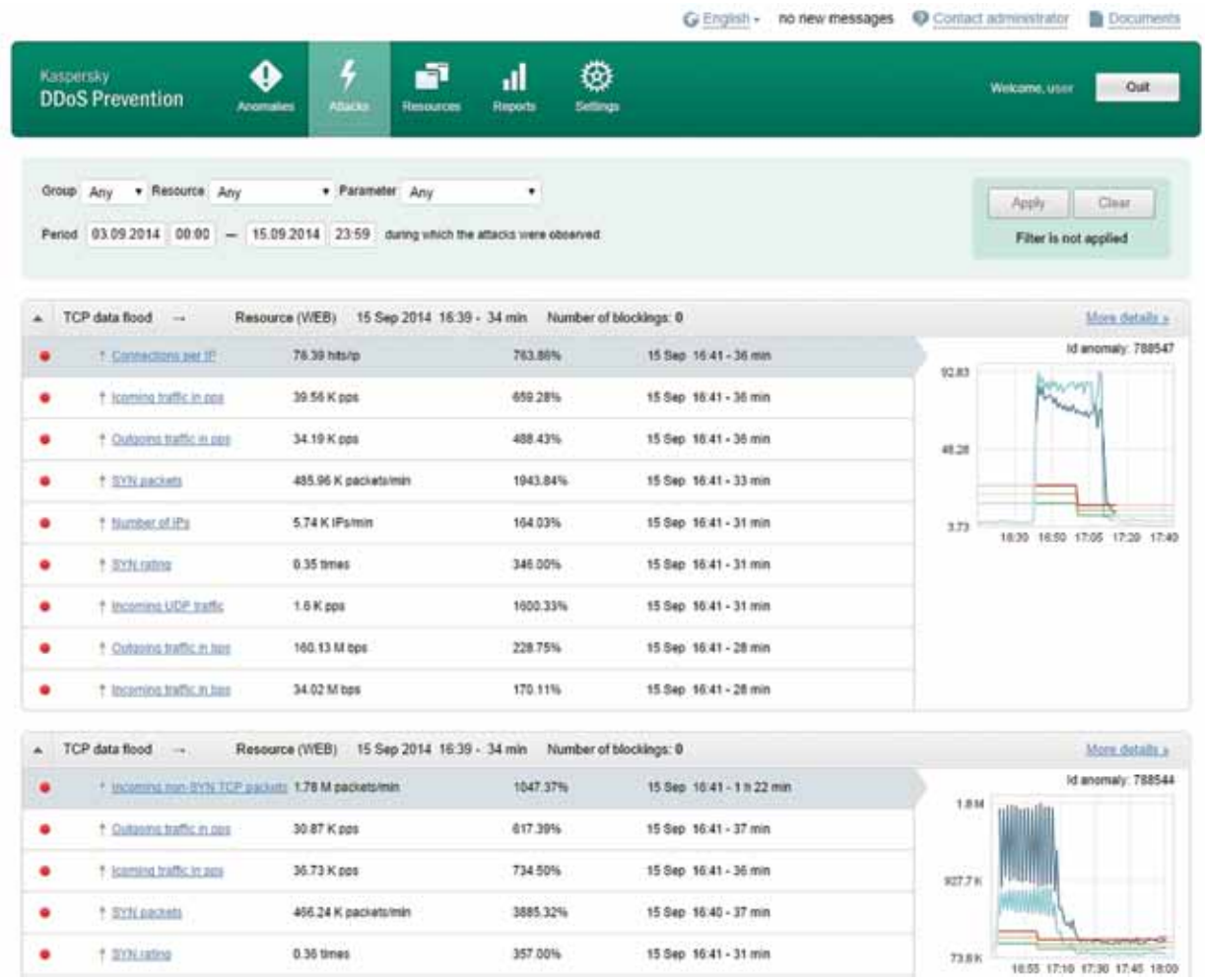
Nasıl çalışır?

Normal koşullarda, İnternet'ten gelen tüm trafik doğrudan müşteriye gider. Koruyucu işlemler, sensörden sinyal alınır alınmaz başlatılır. Bazı durumlarda, Kaspersky Lab'in analistleri bir saldırıyı başlar başlamaz tespit eder ve müşteriyi bilgilendirirler. Bu durumda, tedbir amaçlı önlemler önceden alınabilir. Kaspersky Lab'de görev başında olan DDoS uzmanı, müşteriye ulaşan trafiğin istatistiksel profille eşleşmediğine dair bir sinyal alır. Saldırı doğrulandığı takdirde müşteriye bildirilir ve trafiği temizlik merkezlerine yönlendirmek üzere emir vermesi gerekir (bazı durumlarda, yönlendirmenin otomatik olarak başlatılmasına dair müşteriyle bir anlaşma olur.)

Kaspersky Lab'in teknolojileri saldırının türünü belirler belirlemez, bu saldırı türüne ve belirli web kaynağına özel temizlik kuralları uygulanır. En basit saldırı türlerini yenmek üzere tasarlanmış olan bu kuralların bazıları, sağlayıcının altyapısına iletilir ve sağlayıcının sahip olduğu yönlendiricilerde uygulanır. Kalan trafik, temizlik merkezinin sunucularına iletilir ve IP adresleri, coğrafi veriler, HTTP başlık bilgilerinden edinilen bilgiler, protokollerin doğruluğu ve SYN paketlerinin alışverişi gibi bir dizi karakteristik işarete göre filtrelenir.

Sensör, müşteriye geldikçe trafiği izlemeye devam eder. Bir DDoS saldırısının belirtilerini göstermeye devam ediyorsa sensör temizlik merkezini uyarır ve trafik, derin davranış ve imza analizinden geçer. Bu yöntemler sayesinde, kötü amaçlı trafik imzalara dayalı olarak filtrelenebilir. Örneğin, belirli bir trafik türü tamamen engellenebilir veya IP adresleri, gözlemlenen belirli kriterler temelinde engellenebilir. Böylece, HTTP sel saldırısı dahil olmak üzere en karmaşık saldırılar bile filtrelenir. Bu saldırılar, bir web sitesini ziyaret eden kullanıcının taklitlerini içerir; ancak aslında kaotik, doğal olmayacak kadar hızlıdır ve genellikle zombi bilgisayarlardan gelir.

Kaspersky Lab uzmanları, özel bir arayüz kullanarak bütün süreci izlemektedir. Bir saldırının normalden daha karmaşık veya atipik olması durumunda, bir uzman müdahale edebilir, filtreleme kurallarını değiştirebilir ve süreçleri yeniden düzenleyebilir. Müşteriler de kendi arayüzlerini kullanarak çözümün performansını ve trafiğin davranışını izlerler.



Şekil 3. Müşteri arayüzünün ekran görüntüsü

Saldırı sona erdiğinde, trafik yeniden müşterinin sunucularına yönlendirilir. Kaspersky DDoS Koruması bekleme moduna döner ve müşteriye saldırıya dair, nasıl geliştiğinin ayrıntılı hesabı, ölçülebilir parametreleri anlatan grafikler ve saldırı kaynaklarının coğrafi konumu dahil olmak üzere ayrıntılı bir rapor sunulur.

Kaspersky Lab yaklaşımının avantajları

- Bir saldırı sırasında trafiği yalnızca Kaspersky Lab temizlik merkezlerine yönlendirmek ve sağlayıcı tarafında trafiği filtrelemek, müşterinin maliyeti büyük ölçüde azaltmasına yardımcı olur.
- Filtreleme kuralları, korunması gereken belirli çevrimiçi hizmetlere bağlı olarak her müşteri için bireysel olarak geliştirilir.
- Kaspersky Lab uzmanları, süreci izler ve gerektiğinde filtreleme kurallarını hızlıca düzenlerler.
- Kaspersky DDoS Koruması uzmanları ile Kaspersky Lab geliştiricileri arasındaki yakın işbirliği, çözümün değişen durumlara yanıt olarak esnek ve hızlı bir şekilde adapte edilmesini mümkün kılmaktadır.
- Kaspersky Lab, en yüksek güvenilirlik düzeyini sağlamak amacıyla yalnızca Avrupa ekipmanlarını ve Avrupa ülkelerindeki hizmet sağlayıcılarını kullanır.
- Bu teknolojiyi Rusya'da uygulayarak zengin bir deneyim biriktirmiş olan Kaspersky Lab, önde gelen finansal kuruluşları, ticari ve devlet kurumlarını, çevrimiçi mağazaları vb. başarıyla korumaktadır.

March 15/Global

KASPERSKY lab

www.kaspersky.com