KASPERSKY DDoS PROTECTION

Uw bedrijf beschermen tegen financiële schade en reputatieschade met Kaspersky DDoS Protection

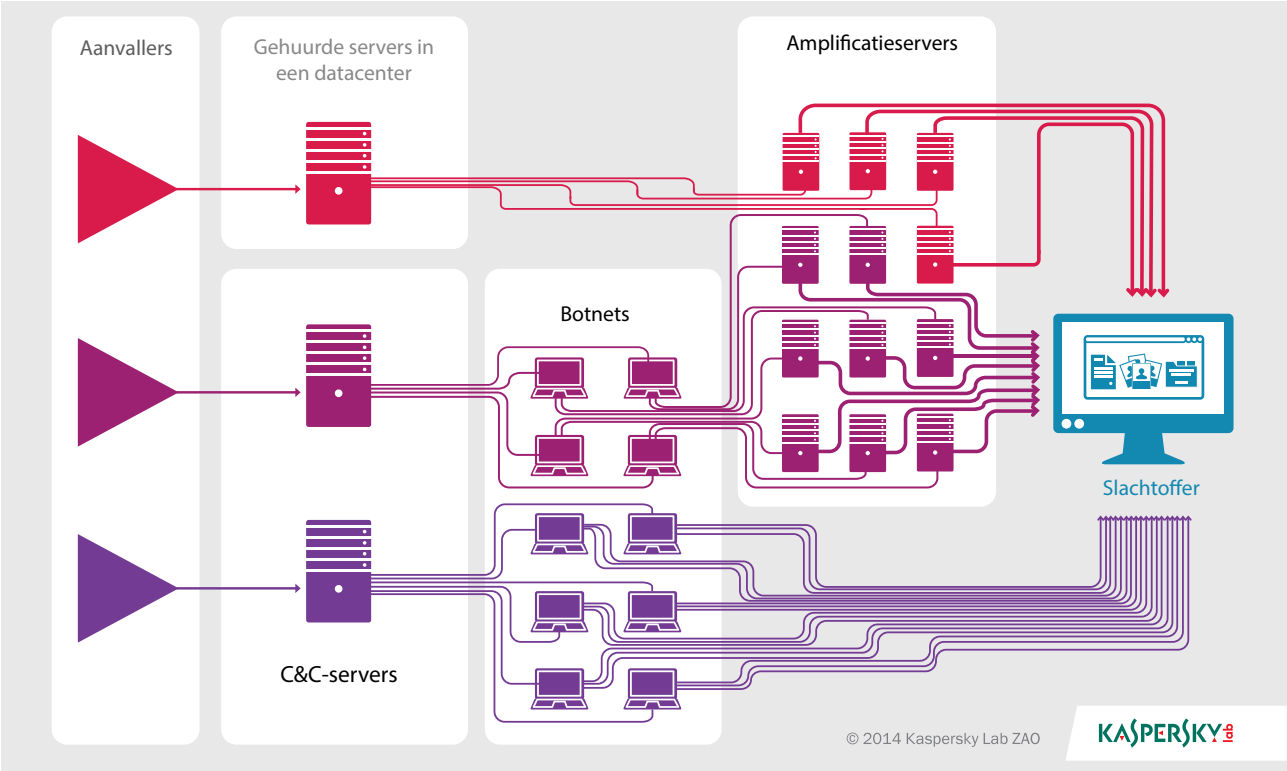
Een DDoS-aanval (Distributed Denial of Service) is een van de populairste wapens in het arsenaal van cybercriminelen. Het doel is de normale toegang tot informatiesystemen zoals websites of databases voor reguliere gebruikers onmogelijk te maken. Er kunnen verschillende motieven achter DDoS-aanvallen zitten, uiteenlopend van cybervandalisme tot gemene concurrentie of zelfs afpersing.

De hedendaagse DDoS-industrie is een structuur met meerdere lagen. Er zitten mensen bij die opdracht geven voor de aanvallen, de botnet-ontwikkelaars die hun bronnen beschikbaar stellen, tussenpersonen die de aanvallen regelen en met de klanten praten, en de mensen die de betalingen regelen voor alle geleverde diensten. Elke netwerknode die via internet beschikbaar is, kan doelwit worden: een specifieke server, een netwerkapparaat of een ongebruikt adres in het subnetwerk van het slachtoffer.

Er zijn twee gebruikelijke scenario's voor de uitvoering van DDoS-aanvallen: verzoeken rechtstreeks verzenden naar de aangevallen bron vanaf een groot aantal bots, of een DDoS-amplificatie-aanval uitvoeren via openbaar beschikbare servers met softwarevulnerability's. In het eerste scenario veranderen cybercriminelen talloze computers in op afstand bestuurde “zombies” die vervolgens de opdrachten van de meester uitvoeren en gelijktijdig verzoeken naar het computersysteem van het slachtoffer sturen (een “gedistribueerde aanval” uitvoeren). Soms wordt een groep gebruikers geworven door hacktivisten, worden zij voorzien van speciale software om DDoS-aanvallen mee uit te voeren en krijgen zij de opdracht om een doelwit aan te vallen.

In het tweede scenario, met een amplificatie-aanval, kunnen servers worden gebruikt die vanuit een datacenter worden verhuurd, in plaats van bots. Openbare servers met kwetsbare software worden vaak gebruikt voor uitbreiding. Tegenwoordig zijn DNS-servers (Domain Name System) of NTP-servers (Network Time Protocol) te gebruiken. Amplificatie van een aanval vindt plaats door retour-IP-adressen te vervalsen (spoofen) en aan een server een kort verzoek te sturen, waarvoor een veel langere reactie vereist is. De ontvangen reactie wordt naar het vervalste IP-adres van het slachtoffer gestuurd.

Scenario's voor DDoS-aanvallen



Afbeelding 1. Stroomdiagram met de populairste versies van DDoS-aanvallen

Er is nog een factor die de situatie nog gevaarlijker maakt. Omdat er overal zoveel malware is en cybercriminelen zoveel botnets hebben gemaakt, kan bijna iedereen een dergelijke aanval uitvoeren. Cybercriminelen adverteren hun services met de boodschap dat iedereen een bepaalde website kan platleggen voor slechts USD 50 per dag. De betalingen vinden doorgaans plaats in cryptovaluta, zodat het vrijwel onmogelijk is de orders via cashflows te achterhalen.

Door de betaalbare prijzen kan elke onlinebron het doelwit worden van een DDoS-aanval. Dit is niet beperkt tot de internetbronnen van grote en bekende organisaties. Het is moeilijker om schade aan te brengen aan webbronnen van grote ondernemingen, maar als deze onklaar worden gemaakt, zijn de kosten van downtijd veel hoger. Los van de directe verliezen door gemiste omzetkansen (zoals onlineverkoop), riskeren bedrijven boetes als ze niet aan hun verplichtingen voldoen, of maken ze kosten voor extra maatregelen om zich te beschermen tegen verdere aanvallen. Tot slot kan het imago van de onderneming worden geschaad, wat bestaande of toekomstige klanten kan kosten.

De totale kosten zijn afhankelijk van de omvang van het bedrijf, de branche en het type service dat wordt aangevallen. Volgens berekeningen door analysebedrijf IDC kan een uur downtijd van een onlineservice een bedrijf USD 10.000 - 50.000 kosten.

Methoden om DDoS-aanvallen te weren

Er zijn talloze bedrijven die services ter bescherming tegen DDoS-aanvallen bieden. Sommige installeren voorzieningen in de informatie-infrastructuur van de klant, sommige gebruiken mogelijkheden binnen ISP-providers en andere kanaliseren verkeer via speciale cleaning centers. Al die oplossingen volgen echter hetzelfde principe: spamverkeer, ofwel verkeer veroorzaakt door cybercriminelen, wordt uitgefilterd.

Het installeren van filterapparatuur aan de klantzijde wordt als de minst effectieve methode beschouwd. Ten eerste is er speciaal opgeleid personeel binnen het bedrijf voor nodig om de apparatuur te onderhouden en de werking ervan aan te passen, wat extra kosten met zich brengt. Ten tweede is het alleen effectief tegen aanvallen op de service, en voorkomt het geenszins aanvallen die het internetkanaal blokkeren. Een werkende service is nutteloos als die niet via het net toegankelijk is. Nu DDoS-aanvallen met amplificatie populairder worden, is het veel eenvoudiger geworden om een verbindingskanaal te overbelasten.

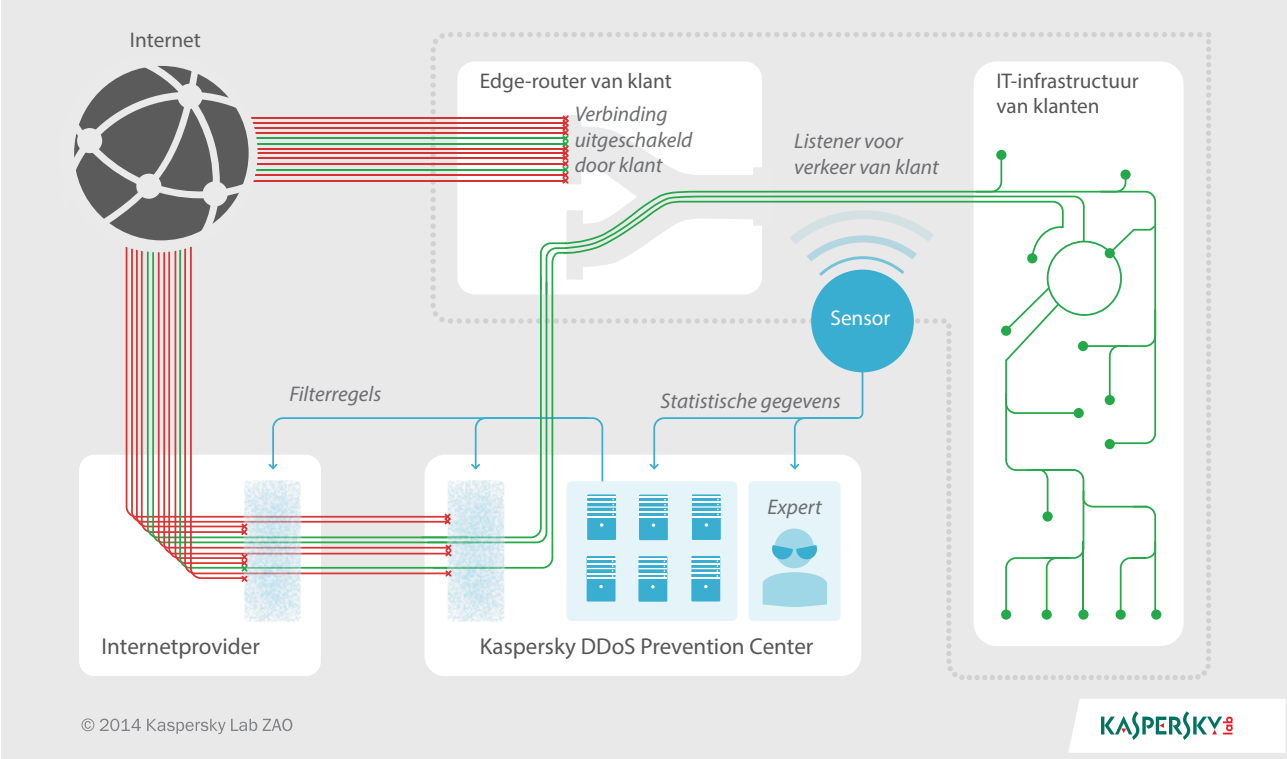
Het verkeer laten filteren door de provider is betrouwbaarder, aangezien er een breder internetkanaal is dat veel moeilijker te blokkeren is. Aan de andere kant zijn providers geen specialisten in beveiligingsservices en filteren ze alleen het meest voor de hand liggende spamverkeer eruit. Subtielere aanvallen gaan aan hen voorbij. Voor een zorgvuldige analyse van een aanval en een snelle reactie zijn de juiste expertise en ervaring vereist. Bovendien maakt deze vorm van bescherming de klant afhankelijk van een specifieke provider en ontstaan er moeilijkheden als de klant een tweede gegevenskanaal moet gebruiken of van provider moet veranderen.

Gespecialiseerde verwerkingscentra die een combinatie van verschillende methoden van verkeersfiltering hanteren, worden beschouwd als effectiefste manier om DDoS-aanvallen onschadelijk te maken.

Kaspersky DDoS Protection

Kaspersky DDoS Protection is een oplossing die bescherming biedt tegen alle typen DDoS-aanvallen door een gedistribueerde infrastructuur van data cleaning centers te gebruiken. In de oplossing worden verschillende methoden gecombineerd, waaronder verkeersfiltering aan de providerzijde, installatie van een op afstand bestuurde voorziening om het verkeer te analyseren naast de infrastructuur van de klant, en het gebruik van gespecialiseerde cleaning centers met flexibele filters. Daarnaast wordt het werk van de oplossing voortdurend bewaakt door experts van Kaspersky Lab, zodat de inzet van een aanval zo snel mogelijk wordt gedetecteerd en filters naar wens kunnen worden aangepast.

Kaspersky DDoS Protection in actieve modus



Afbeelding 2. Kaspersky DDoS Protection: werkingsdiagram

Arsenaal van Kaspersky Lab

Kaspersky Lab pakt al ruim tien jaar met succes een breed scala aan onlinedreigingen aan. In die periode hebben analisten van Kaspersky Lab een uniek expertiseniveau verworven, waaronder een gedetailleerd inzicht in de werking van DDoS-aanvallen. De experts van het bedrijf houden de nieuwste ontwikkelingen op internet voortdurend in de gaten, analyseren de nieuwste methoden voor de uitvoering van cyberaanvallen en verbeteren onze bestaande beveiligingstools. Met deze expertise op zak is het mogelijk een DDoS-aanval te detecteren zodra die wordt uitgevoerd en voordat die de beoogde webbron overspoelt.

Het tweede element in de Kaspersky DDoS Protection-technologie is een sensor die naast de IT-infrastructuur van de klant wordt geïnstalleerd. De sensor bestaat uit software die onder het Ubuntu-besturingssysteem wordt uitgevoerd en waarvoor een gewone x86-server vereist is. Deze analyseert de gebruikte typen protocollen, het verzonden aantal bytes en gegevenspakketten, het gedrag van de klant op de website (de metagegevens), of informatie over de verzonden gegevens. Er wordt geen verkeer omgeleid of gewijzigd, en geen inhoud van berichten geanalyseerd. De statistieken worden vervolgens naar de Kaspersky DDoS Protection-infrastructuur in de cloud gestuurd, waar een op statistieken gebaseerd profiel wordt gemaakt voor elke klant, op basis van de verzamelde metagegevens. In wezen zijn deze profielen records van typische informatie-uitwisselingspatronen voor elke klant. Veranderingen in gangbare gebruikstijden worden geregistreerd. Later wordt het verkeer geanalyseerd. Telkens wanneer het gedrag van het verkeer anders is dan het op statistieken gebaseerde profiel, kan er sprake zijn van een aanval.

De cleaning centers vormen de sluitsteen van Kaspersky DDoS Protection. Ze bevinden zich op de voornaamste internet-backbone-lijnen, in plaatsen zoals Frankfurt en Amsterdam. Kaspersky Lab gebruikt gelijktijdig verschillende cleaning centers, zodat het verkeer voor filtering kan worden verdeeld of omgeleid. De verwerkingscentra zijn verenigd in een gemeenschappelijke informatie-infrastructuur in de cloud en de gegevens bevinden zich binnen die grenzen. Het webverkeer van Europese klanten verlaat bijvoorbeeld niet het Europese grondgebied.

Nog een belangrijke manier om DDoS-verkeer te beheersen is het aan de providerzijde te filteren. De ISP levert niet alleen een internetkanaal, deze kan ook een technologiepartnerschap met Kaspersky Lab aangaan. Kaspersky DDoS Protection kan dan het duidelijkste spamverkeer, gebruikt in de meeste DDoS-aanvallen, zo dicht mogelijk bij de bron tegenhouden. Zo wordt samenvoeging van de streams tot één krachtige aanval voorkomen en worden de cleaning centers ontzien. Die blijven dan beschikbaar voor de afhandeling van geavanceerder spamverkeer.

Tools voor verkeersomleiding

De eerste essentiële vereiste voor een effectieve beveiligingsoplossing is het instellen van een verbindingskanaal tussen de cleaning centers en de IT-infrastructuur van de klant. In Kaspersky DDoS Protection zijn deze kanalen gerangschikt volgens het GRE-protocol (Generic Routing Encapsulation). Hiermee wordt een virtuele tunnel gemaakt tussen het cleaning center en de netwerkapparatuur van de klant, waardoor het schone verkeer aan de klant wordt geleverd.

De feitelijke omleiding kan via twee methoden plaatsvinden: door het subnet van de klant aan te kondigen via een BGP-protocol voor dynamische routering, of door de DNS-record te wijzigen met de introductie van de URL van het cleaning center. De eerste methode heeft de voorkeur omdat hiermee verkeer veel sneller kan worden omgeleid en bescherming kan worden geboden tegen aanvallen die rechtstreeks zijn gericht op een specifiek IP-adres. Bij deze methode moet de klant echter wel een reeks adressen hebben dat onafhankelijk is van de provider, zoals een blok IP-adressen dat is geleverd door een regionaal internetregistratiebureau.

Wat de feitelijke omleidingsprocedure betreft, is er weinig verschil tussen de twee methoden. Als de eerste methode wordt gebruikt, maken de BPG-routers aan de klantzijde en in het cleaning center een permanente verbinding via de virtuele tunnel. In het geval van een aanval wordt een nieuwe route gemaakt vanaf het cleaning center naar de klant. Bij gebruik van de tweede methode krijgt de klant een IP-adres toegewezen uit de adresgroep van het cleaning center. Als er een aanval begint, vervangt de klant het IP-adres in de DNS A-record door het IP-adres dat is toegewezen door het cleaning center. Daarna wordt al het verkeer dat op het adres van de klant binnenkomt eerst naar het cleaning center gestuurd. Om de aanval op het oude IP-adres te stoppen, moet de provider echter al het inkomende verkeer blokkeren behalve de gegevens die afkomstig zijn van het cleaning center.

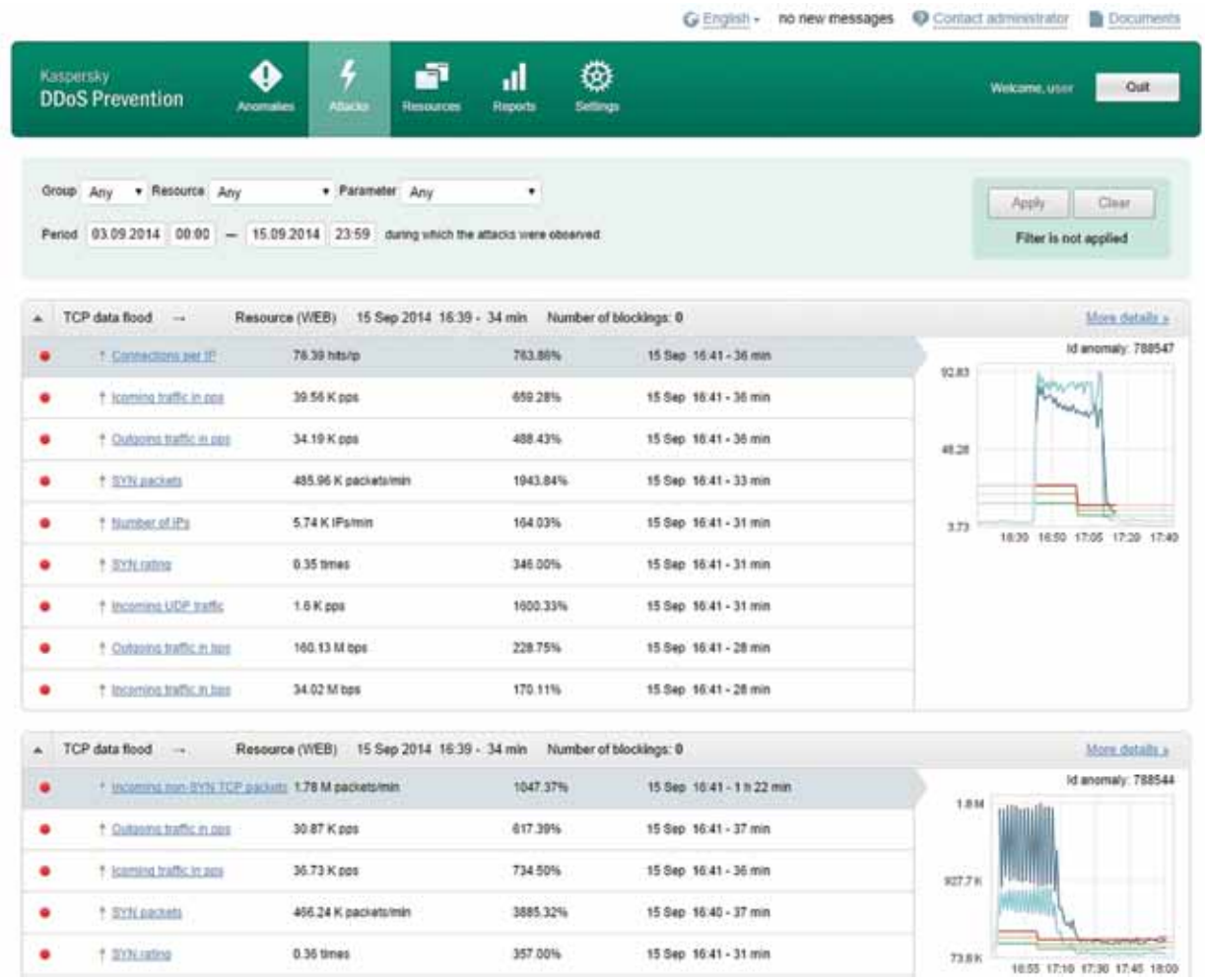
Hoe het werkt

In normale omstandigheden gaat al het verkeer van internet direct naar de klant. De beschermende acties beginnen zodra een signaal van de sensor binnenkomt. In sommige gevallen merken analisten van Kaspersky Lab een aanval zodra die begint en stellen zij de klant op de hoogte. In dit geval kunnen vooraf preventieve maatregelen worden genomen. De dienstdoende DDoS-expert bij Kaspersky Lab ontvangt een signaal dat inkomend verkeer bij de klant niet overeenkomt met het statistische profiel. Als de aanval wordt bevestigd, krijgt de klant een melding van de aanval en moet de klant de opdracht geven om het verkeer om te leiden naar de cleaning centers (in sommige gevallen kan er een overeenkomst met de klant zijn dat het omleiden automatisch start).

Zodra het type aanval is vastgesteld met de technologieën van Kaspersky Lab, worden specifieke schoonmaakregels toegepast voor dit type aanval en de specifieke webbron. Sommige regels, ontworpen om de meest ongerichte aanvalstypen tegen te gaan, worden gecommuniceerd naar de infrastructuur van de provider en toegepast op routers die eigendom zijn van de provider. Het overige verkeer gaat naar de servers van het cleaning center en wordt gefilterd op basis van een aantal kenmerken, zoals IP-adressen, geografische gegevens, informatie uit de HTTP-headers, de juistheid van protocollen, uitwisseling van SYN-pakketten enzovoort.

De sensor blijft het verkeer bewaken dat bij de klant aankomt. Als er nog steeds tekenen van een DDoS-aanval zijn, waarschuwt de sensor het cleaning center en worden het gedrag en de definitie van het verkeer grondig geanalyseerd. Met deze methoden kan schadelijk verkeer worden uitgefilterd op basis van definities, dat wil zeggen: een specifiek type verkeer kan volledig worden geblokkeerd, of IP-adressen kunnen worden geblokkeerd op basis van specifieke waargenomen criteria. Op deze manier worden zelfs de meest geavanceerde aanvallen gefilterd, inclusief een aanvallen waarbij een HTTP-adres wordt overspoeld. Bij deze aanvallen worden gebruikers nagebootst die een website bezoeken. Het bezoek verloopt echter chaotisch en onnatuurlijk snel, en is doorgaans afkomstig van een horde zombiecomputers.

De experts van Kaspersky Lab bewaken het hele proces met behulp van een speciale interface. Als een aanval complexer of ongebruikelijk is, kan de expert ingrijpen, de filterregels wijzigen en de processen opnieuw organiseren. Klanten kunnen via hun eigen interface ook zien hoe de oplossing presteert en hoe het verkeer zich gedraagt.



Afbeelding 3. Schermafbeelding van de interface van de klant

Wanneer de aanval voorbij is, wordt het verkeer teruggeleid naar de servers van de klant. Kaspersky DDoS Protection keert terug naar de stand-bymodus en de klant ontvangt een gedetailleerd rapport van de aanval, inclusief een uitgebreid verslag van de ontwikkeling, grafieken met gemeten parameters en de geografische verspreiding van de aanvalsbronnen.

Voordelen van de aanpak van Kaspersky Lab

- Alleen omleiding van verkeer naar cleaning centers van Kaspersky Lab tijdens een aanval en filtering van verkeer aan de providerzijde, leiden tot aanzienlijke kostenverlaging voor de klant.
- Filterregels worden voor elke klant afzonderlijk ontwikkeld, afhankelijk van de specifieke onlineservices die moeten worden beschermd.
- Experts van Kaspersky Lab bewaken het proces en passen filterregels indien nodig snel aan.
- Dankzij nauwe samenwerking tussen experts van Kaspersky DDoS Protection en ontwikkelaars van Kaspersky Lab kan de oplossing flexibel en snel worden aangepast aan veranderende omstandigheden.
- Voor de hoogst mogelijke graad van betrouwbaarheid gebruikt Kaspersky Lab alleen Europese apparatuur en serviceverleners in Europese landen.
- Kaspersky Lab heeft een schat aan ervaring opgedaan met de toepassing van deze technologie in Rusland, waar het bedrijf toonaangevende financiële instellingen, commerciële bedrijven, overheidsinstanties, onlinewinkels en dergelijke met succes beschermt.

15 maart/Global