KASPERSKY lab

Schutz Ihres Unternehmens vor finanziellen Verlusten und Rufschädigung mit Kaspersky DDoS Protection

Distributed-Denial-of-Service-Angriffe (DDoS) gehören zu den beliebtesten Waffen im Arsenal von Cyberkriminellen. Sie zielen darauf ab, den Betrieb von Informationssystemen wie Websites oder Datenbanken lahmzulegen bzw. zu stören. Hinter dieser Art von Angriff können unterschiedliche Motive stehen, die vom Cyber-Vandalismus über unlautere Wettbewerbspraktiken bis hin zu Erpressung reichen.

DDoS-Angriffe finden heutzutage in einem komplexen Geflecht aus geschäftlichen Beziehungen statt. Hinter dem eigentlich Auftraggeber steht eine ganze Reihe beteiligter Personen: die Erschaffer der Botnetze, die ihre Infrastruktur zur Verfügung stellen, Zwischenhändler, welche die Angriffe arrangieren und den Kontakt zu den Auftraggebern halten, und schließlich noch eine weitere Gruppe, welche die finanzielle Vergütung für die geleisteten Dienste organisiert. Jeder Netzwerk-Node im Internet kann zum Ziel werden, egal ob es sich um einen bestimmten Server, ein Netzwerkgerät oder eine nicht mehr genutzte Adresse im Teilnetzwerk des Opfers handelt.

Bei der Ausführung von DDoS-Angriffen haben sich zwei beliebte Vorgehensweisen herauskristallisiert: die direkte Übermittlung von gleichzeitigen Anfragen über eine riesige Anzahl so genannter Bots an die angegriffene Ressource oder das Einleiten eines DDoS-Verstärkungsangriffs über öffentliche Server mit Software-Schwachstellen. Im ersten Szenario wird eine Vielzahl von Computern in ferngesteuerte „Zombies“ verwandelt, die dann den Befehlen ihres Erschaffers folgen und gleichzeitig das angegriffene System mit Anfragen überschwemmen (ein so genannter „verteilter Angriff“). Manchmal wird auch eine Gruppe von Benutzern von Hacktivisten rekrutiert, mit spezieller DDoS-Software ausgestattet und dann beauftragt, ein bestimmtes Ziel anzugreifen.

Beim Verstärkungsangriff werden anstelle eines Botnetzes Server eingesetzt, die eigens von einem Rechenzentrum gemietet wurden. Öffentliche Server mit anfälliger Software werden häufig zur Verstärkung eingesetzt. Heutzutage werden dafür in der Regel DNS- (Domain Name System) oder NTP-Server (Network Time Protocol) genutzt. Angriffe werden durch zwei Methoden verstärkt: entweder durch das Fälschen von IP-Rückgabeadressen oder das Senden eines kurzen Datenpakets, das von dem angegriffenen Server mit einem sehr langen Paket beantwortet werden muss. Die empfangene Antwort wird dann an die gefälschte IP-Adresse weitergeleitet, die zum Angriffsziel gehört.

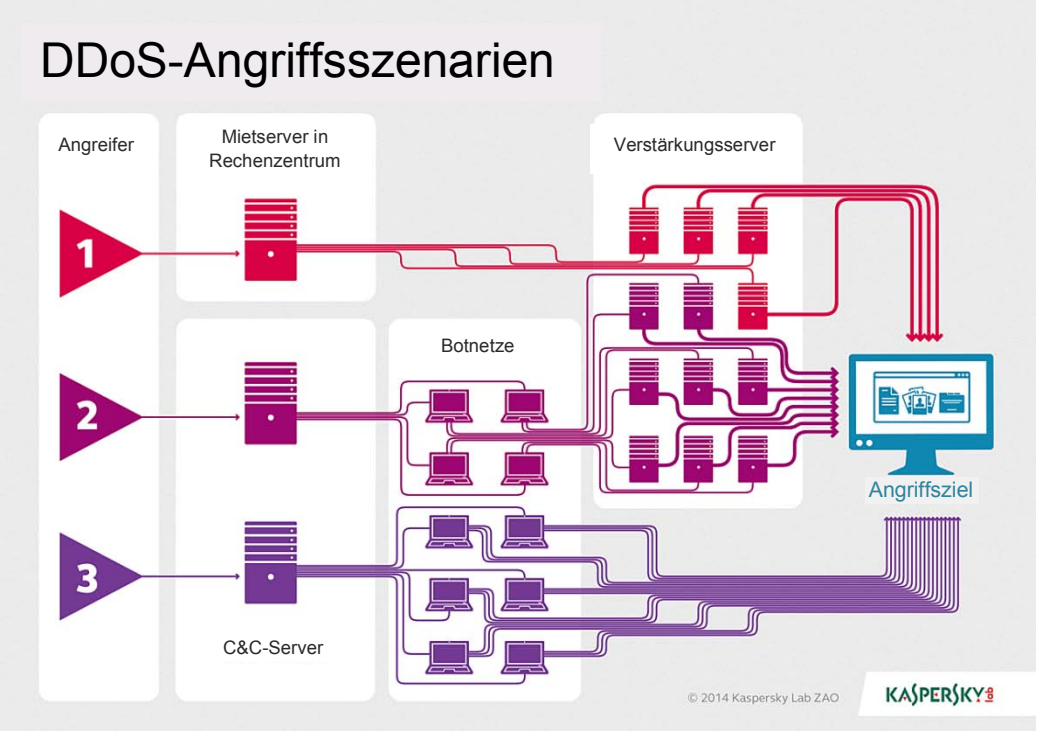

Abbildung 1: Schematische Darstellung weit verbreiteter DDoS-Angriffsmethoden

Es gibt einen weiteren Faktor, der das Risikopotenzial der Situation zusätzlich erhöht. Aufgrund der riesigen Menge an Malware, die im Umlauf ist, und des großen Angebots von Botnetzen, die von Cyberkriminellen aufgebaut wurden, kann praktisch jeder einen DDoS-Angriff in Auftrag geben. Online-Kriminelle bieten den Service, eine bestimmte Website auszuschalten, schon für 50 US-Dollar am Tag an. Da die Zahlungen in der Regel in so genannter Kryptowährung erfolgen, ist es so gut wie unmöglich, die Finanzströme zurückzuverfolgen.

Die erschwinglichen Preise bedeuten, dass jede Online-Ressource zum Ziel eines DDoS-Angriffs werden kann, nicht nur die Internetpräsenzen großer und angesehener Unternehmen. Es ist zwar schwieriger, die Web-Ressourcen von Konzernen zu treffen, wenn sie jedoch lahmgelegt werden, dann sind die Kosten eines solchen Ausfalls umso höher. Abgesehen von den direkten Verlusten durch entgangene Geschäfte (z. B. elektronische Verkäufe) müssen Unternehmen mit Strafgebühren rechnen, da sie ihren Verpflichtungen nicht nachkommen konnten, oder mit Kosten für zusätzliche Sicherheitsmaßnahmen, um sich gegen künftige Angriffe zu rüsten. Nicht zuletzt kann auch der Ruf eines Unternehmens Schaden nehmen, was zum Verlust vorhandener oder zukünftiger Kunden führen kann.

Der Gesamtschaden hängt von der Größe des Unternehmens, der jeweiligen Branche und der Art des Services ab, der angegriffen wird. Laut Berechnungen von IDC, einem Marktforschungsunternehmen, kann eine einstündige Ausfallzeit bei einem Online-Service ein Unternehmen bereits 10.000 bis 50.000 US-Dollar kosten.

Maßnahmen zur Verteidigung gegen DDoS-Angriffe

Es gibt Dutzende Unternehmen am Markt, die Services zum Schutz vor DDoS-Angriffen anbieten. Einige von ihnen installieren Appliances in der IT-Struktur des Kunden, andere nutzen bei Internetdienstanbietern vorhandene Funktionen und wieder andere leiten den Datenverkehr durch spezielle Rechenzentren um, in denen er bereinigt wird. All diesen Verfahren liegt jedoch dasselbe Prinzip zugrunde: der Datenschrott, d. h. der in krimineller Absicht generierte Datenverkehr, soll herausgefiltert werden.

Die Installation einer Filtereinrichtung auf Seiten des Kunden gilt als die am wenigsten effektive Methode. Erstens sind für die Konfiguration und Bedienung der Geräte speziell geschulte Mitarbeiter im Unternehmen erforderlich, wodurch zusätzliche Kosten entstehen, und zweitens zeigt die Methode nur bei Angriffen auf den jeweiligen Service Wirkung, nicht aber bei Angriffen, welche die Internetverbindung lahmlegen. Ein funktionierender Service hat keinerlei Nutzen, wenn er über das Internet nicht erreichbar ist. Mit der zunehmenden Verbreitung von DDoS-Verstärkungsangriffen ist es weitaus einfacher geworden, eine Internetanbindung zu überlasten.

Den Datenverkehr vom Internetdienstanbieter filtern zu lassen, ist effektiver, da die Internetanbindung dort über eine höhere Bandbreite verfügt und so schwieriger zu überlasten ist. Andererseits besitzen die meisten Internetdienstanbieter keine speziellen Sicherheitseinrichtungen und filtern lediglich den offensichtlichen Datenmüll heraus, wodurch raffinierte Angriffe oft unbemerkt bleiben. Für eine eingehende Analyse eines Angriffs und eine umgehende Reaktion sind entsprechende Expertise und Erfahrung erforderlich. Außerdem macht die oben genannte Art der Verteidigung den Kunden von einem bestimmten Internetdienstanbieter abhängig, was zu Schwierigkeiten führt, wenn er bei einem Ausfall auf eine andere Datenanbindung zurückgreifen muss oder den Anbieter wechseln möchte.

Die effektivste Methode zur Neutralisierung von DDoS-Angriffen stellen mithin spezielle Bereinigungszentren dar, die mit einer Kombination aus unterschiedlichen Methoden zur Datenfilterung arbeiten.

Kaspersky DDoS Protection

Kaspersky DDoS Protection ist eine Lösung, die auf einer verteilten Struktur aus Datenbereinigungszentren basiert und effektiven Schutz vor allen möglichen Arten von DDoS-Angriffen bietet. Sie vereint unterschiedliche Methoden, darunter Datenverkehrsfilterung beim Internetdienstanbieter, die Installation einer ferngesteuerten Appliance zur Analyse des Datenverkehrs am Kundenstandort sowie die Nutzung spezieller Bereinigungszentren mit flexiblen Filterverfahren. Außerdem wird die Lösung kontinuierlich von Experten bei Kaspersky Lab überwacht, sodass Angriffe bereits in der Entstehung entdeckt werden und ein frühzeitiges Anpassen der Filter möglich wird.

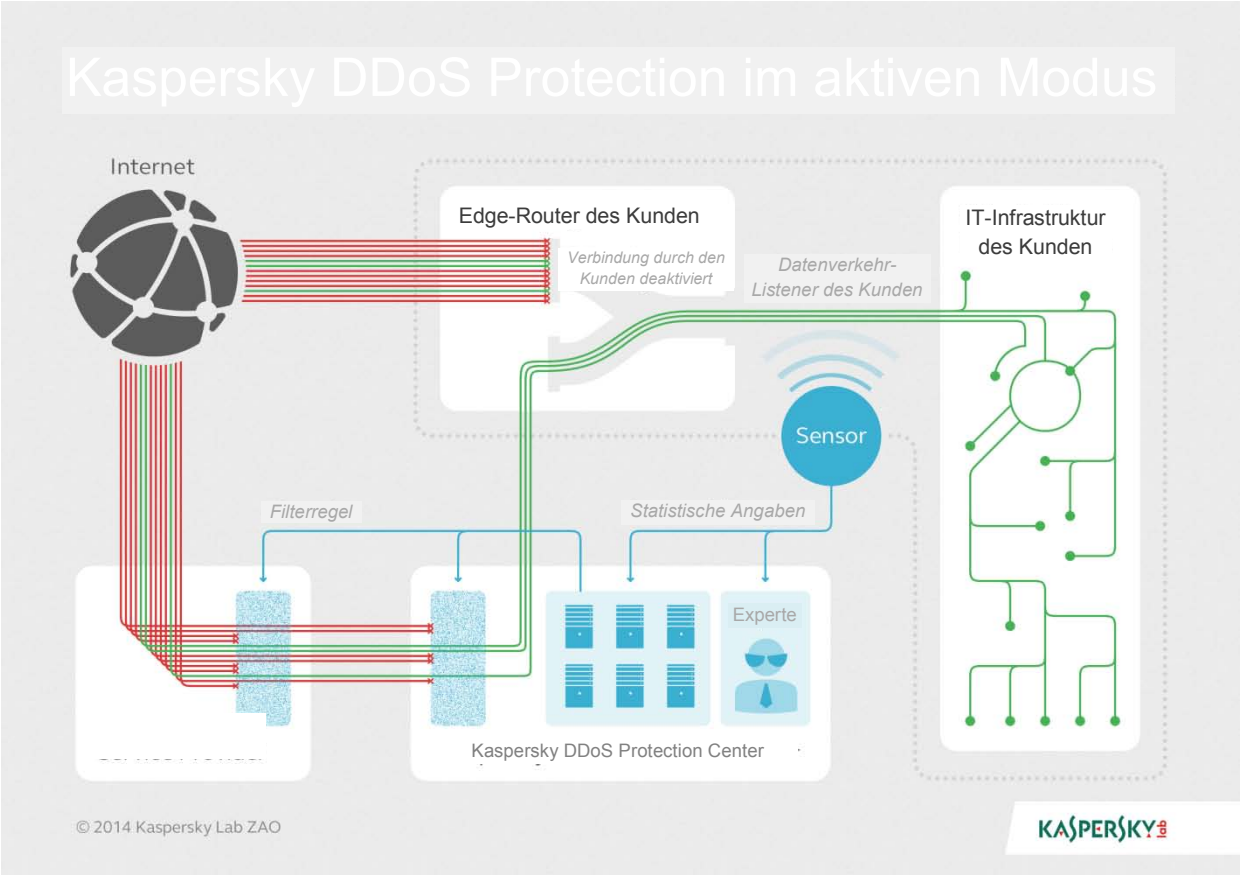

Abbildung 2: Kaspersky DDoS Protection-Ablaufdiagramm

Das Arsenal von Kaspersky Lab

Seit mehr als einem Jahrzehnt hat Kaspersky Lab bei der Bekämpfung von Online-Bedrohungen seine hohe Effektivität unter Beweis gestellt. Unsere Analysten konnten sich dabei ein unvergleichliches Fachwissen aneignen, darunter auch detaillierte Einblicke in die Funktionsweise von DDoS-Angriffen. Unsere Fachleute beobachten ständig die neuesten Entwicklungen im Internet, analysieren aktuelle Cyber-Angriffsmethoden und verbessern vorhandene Verteidigungsmaßnahmen. Dies ermöglicht es uns, einen DDoS-Angriff bereits im Entstehen zu erkennen, noch bevor er die angegriffene Web-Ressource durch Überflutung lahmlegen kann.

Die zweite Hauptkomponente unserer DDoS Protection-Technologie ist ein Sensor, der in unmittelbarer Nähe der IT-Infrastruktur des Kunden installiert wird. Dabei handelt es sich um eine Software, die unter dem Betriebssystem Ubuntu auf einem herkömmlichen x86-Server läuft. Der Sensor analysiert die Art der gesendeten Protokolle, die Anzahl der gesendeten Bytes und Datenpakete sowie das Verhalten des Kunden auf seiner Website, also die Metadaten der gesendeten Pakete. Er leitet den Datenverkehr an keiner Stelle um und ändert oder analysiert auch nicht den Inhalt von Nachrichten. Die Statistiken werden dann an die Cloud-basierte Kaspersky DDoS Protection-Infrastruktur übermittelt, wo für jeden Kunden auf Basis der erfassten Metadaten ein Statistikprofil angelegt wird. Im Grunde handelt es sich bei diesen Profilen um Aufzeichnungen von Datenaustauschmustern, die für jeden der Kunden charakteristisch sind. Treten Änderungen der typischen Nutzungszeiten auf, werden diese aufgezeichnet. Der Datenverkehr wird dann analysiert, wobei jedes Datenverkehrsmuster, das von dem Statistikprofil abweicht, bereits ein Anzeichen für einen Angriff sein kann.

Das Herzstück von Kaspersky DDoS Protection sind seine Datenbereinigungszentren. Diese befinden sich in der Nähe der wichtigsten Internet-Knotenpunkte, z. B. in Städten wie Frankfurt und Amsterdam. Kaspersky Lab nutzt mehrere Zentren gleichzeitig und hat dadurch die Möglichkeit, Datenverkehrsströme aufzuteilen oder umzuleiten. Die Verarbeitungszentren bilden zusammen eine gemeinsame Cloud-basierte IT-Infrastruktur, deren Grenzen die Daten nicht verlassen. Der Webverkehr unserer europäischen Kunden verlässt beispielsweise zu keinem Zeitpunkt Europa.

Eine weitere wichtige Methode zur Kontrolle von DDoS-Datenverkehr ist die Filterung auf Seiten des Internetdienstanbieters. Internetdienstanbieter stellen nicht nur eine Internetanbindung zur Verfügung, es besteht für sie auch die Möglichkeit, eine technologische Partnerschaft mit Kaspersky Lab einzugehen. Auf diese Weise kann Kaspersky DDoS Protection den offensichtlichen Datenmüll, der bei einem Großteil der DDoS-Angriffe verwendet wird, so nahe an der Quelle herausfiltern wie möglich. Dies verhindert das Entstehen eines einzelnen, gewaltigen Datenstroms und verringert die Belastung der Bereinigungszentren, denen so mehr Kapazität für ausgeklügeltere Angriffe bleibt.

Verfahren zur Datenverkehrsumleitung

Von entscheidender Bedeutung für eine effektive Sicherheitslösung ist die Einrichtung eines Kommunikationskanals zwischen den Bereinigungszentren und der IT-Infrastruktur des Kunden. Im Fall von Kaspersky DDoS Protection basieren diese Verbindungen auf dem Generic Routing Encapsulation-Protokoll. Sie bauen einen virtuellen Tunnel zwischen dem Bereinigungszentrum und den Netzwerkgeräten auf Kundenseite auf, durch den der bereinigte Datenverkehr an den Kunden übermittelt wird.

Die eigentliche Datenverkehrsumleitung geschieht dann anhand einer der folgenden Methoden: entweder durch Ankündigung des kundenseitigen Subnetzes mithilfe des BGP-Routingprotokolls oder durch Modifizierung des DNS-Datensatzes, in den die URL des Bereinigungszentrums eingefügt wird. Die erste Methode bietet den Vorteil, dass der Datenverkehr weitaus schneller umgeleitet werden kann und ein wirkungsvoller Schutz bei Angriffen auf einzelne IP-Adressen gewährleistet ist. Für diese Methode benötigt der Kunde jedoch einen Adressbereich, der unabhängig von seinem Internetdienstanbieter ist, z. B. einen IP-Adressblock von einer regionalen Internet-Registrierungsstelle.

In Bezug auf das eigentliche Umleitungsverfahren bestehen zwischen den beiden Methoden keine wesentlichen Unterschiede. Bei der ersten Methode stellen die BPG-Router am Kundenstandort und im Bereinigungszentrum über den virtuellen Tunnel eine permanente Verbindung her. So steht für den Fall eines Angriffs eine zusätzliche Route vom Bereinigungszentrum zum Kunden zur Verfügung. Bei der zweiten Methode wird dem Kunden-Client eine Adresse aus dem IP-Adresspool des Bereinigungszentrums zugewiesen. Bei einem Angriff tauscht der Kunde seine IP-Adresse im DNS-A-Datensatz gegen die ihm zugewiesene IP-Adresse aus. Auf diese Weise wird der gesamte für den Kunden bestimmte Datenverkehr an das Bereinigungszentrum umgeleitet. Um zu verhindern, dass der Angriff auf die alte IP-Adresse weiterläuft, muss der Internetdienstanbieter jedoch den gesamten eingehenden Datenverkehr blockieren – mit Ausnahme der vom Bereinigungszentrum stammenden Daten.

Funktionsweise

Unter normalen Umständen kommt der gesamte Datenverkehr aus dem Internet direkt beim Kunden an. Die Schutzmaßnahmen werden eingeleitet, sobald ein Signal vom Sensor eingeht. Manchmal erfahren die Analysten bei Kaspersky Lab von einem Angriff in dem Augenblick, in dem dieser eingeleitet wird, und informieren den Kunden umgehend. In diesem Fall können schon im Vorfeld Präventivmaßnahmen eingeleitet werden. Der diensthabende DDoS-Experte bei Kaspersky Lab wird benachrichtigt, dass der beim Kunden eingehende Datenverkehr von seinem Statistikprofil abweicht. Bei Bestätigung eines Angriffs wird der Kunde darüber informiert und sollte daraufhin den Auftrag erteilen, den Datenverkehr an die Bereinigungszentren umzuleiten (in einigen Fällen besteht eine Vereinbarung mit dem Kunden, dass die Umleitung automatisch eingeleitet wird).

Sobald Kaspersky Lab den vorliegenden Angriffstyp erkannt hat, kommen spezielle Bereinigungsregeln für den Angriffstyp und die angegriffene Webressource zum Einsatz. Einige der Regeln – vorgesehen für die einfachsten Angriffsformen – werden an die Infrastruktur des Internetdienstanbieters übermittelt und kommen dann auf dessen Routern zum Einsatz. Der übrige Verkehr wird an die Server im Bereinigungszentrum umgeleitet und anhand einer Reihe charakteristischer Merkmale gefiltert, darunter IP-Adressen, geografische Daten, HTTP-Kopfzeilendaten, die Fehlerfreiheit der Protokolle, der Austausch von SYN-Paketen usw.

Der beim Kunden eingehende Datenverkehr wird weiterhin durch den Sensor überwacht. Liegen immer noch Anzeichen eines DDoS-Angriffs vor, alarmiert der Sensor das Bereinigungszentrum, woraufhin der Datenverkehr einer eingehenden Verhaltens- und Signaturanalyse unterzogen wird. Mithilfe dieser Methode lässt sich schädlicher Datenverkehr auf Grundlage von Signaturen herausfiltern, d. h. ein bestimmter Datenverkehrstyp oder IP-Adressen mit speziellen Kriterien können vollständig geblockt werden. Auf diese Weise können selbst die raffiniertesten Angriffe, darunter auch HTTP-Überflutungsangriffe, neutralisiert werden. Diese Angriffe imitieren Benutzer, die eine Website besuchen, sind aber tatsächlich chaotisch, ungewöhnlich schnell und werden in der Regel über Botnetze ausgeführt.

Unsere Experten überwachen den gesamten Vorgang über eine spezielle Benutzeroberfläche. Bei einem außergewöhnlich komplexen oder atypisch verlaufenden Angriff greift der Experte ein, ändert möglicherweise die Filterregeln und stellt den Ablauf um. Auch der Kunde kann das Verhalten unserer Sicherheitslösung und das der Datenströme über eine eigene Benutzeroberfläche verfolgen.

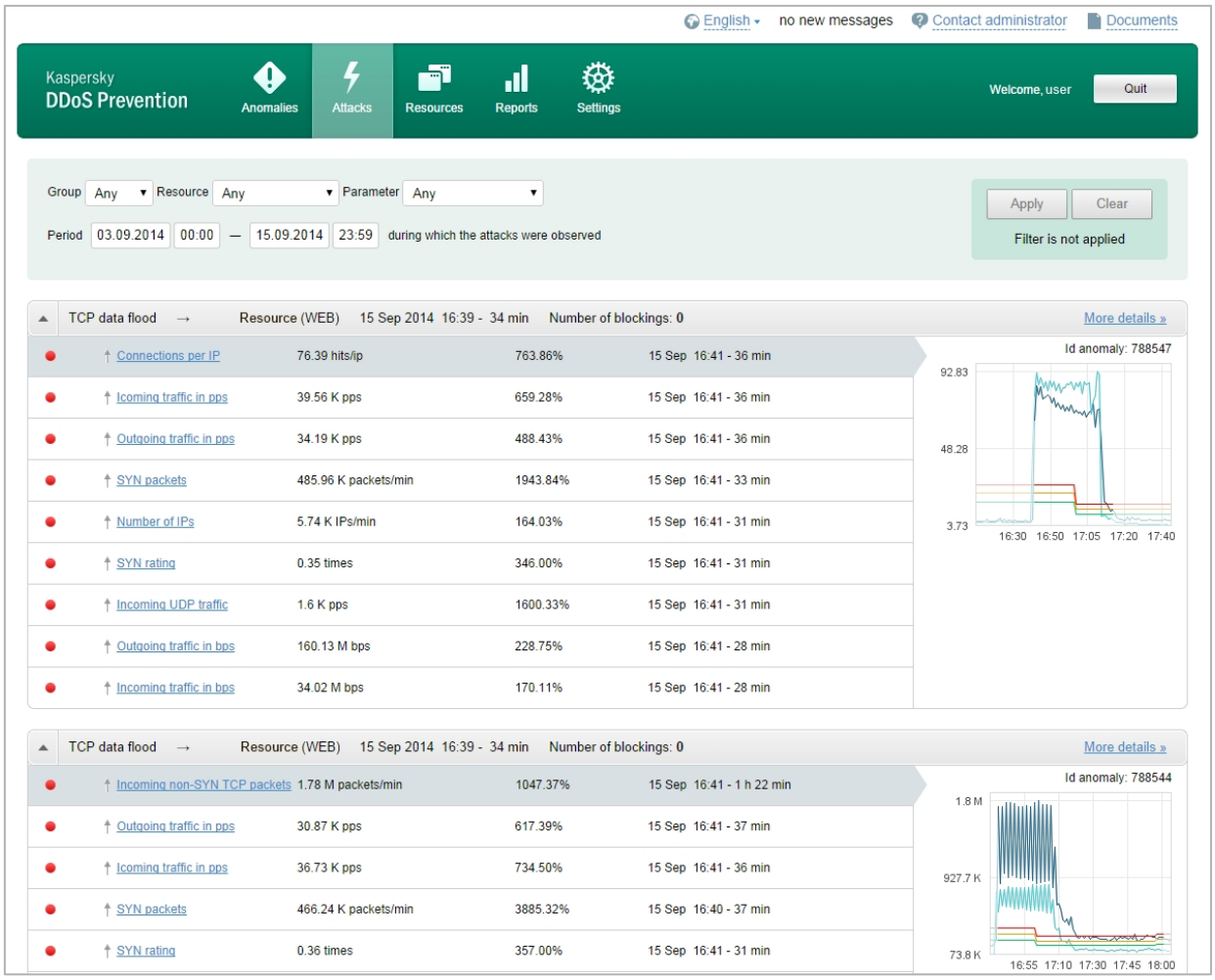

Abbildung 3: Benutzeroberfläche des Kunden

Nach Beendigung des Angriffs wird der Datenverkehr wieder an die Server des Kunden umgeleitet. Kaspersky DDoS Protection schaltet wieder in den Standby-Modus um, und der Kunde erhält einen detaillierten Bericht zum Angriff, inklusive einer ausführlichen Beschreibung des Angriffsverlaufs, einer grafischen Darstellung der messbaren Parameter sowie der geografischen Verteilung der Angriffsquellen.

Vorteile unseres Ansatzes

- Die einzige Methode, die Kosten für den Kunden bei einem Angriff erheblich zu reduzieren, besteht darin, den Datenverkehr an die Bereinigungszentren von Kaspersky Lab umzuleiten und den Datenverkehr beim Internetdienstanbieter zu filtern.
- Die Filterregeln werden individuell für jeden unserer Kunden angepasst und hängen von der Art der Online-Services ab, die geschützt werden sollen.
- Unsere Experten überwachen den Vorgang fortlaufend und modifizieren die Regeln bei Bedarf zeitnah.
- Eine enge Zusammenarbeit zwischen Kaspersky DDoS Protection-Experten und unseren Entwicklern macht es möglich, die Lösung schnell und flexibel an geänderte Umstände anzupassen.
- Um ein Höchstmaß an Zuverlässigkeit zu gewährleisten, nutzt Kaspersky Lab ausschließlich in Europa gefertigte Geräte und Dienstanbieter aus europäischen Ländern.
- Kaspersky Lab hat bei der Nutzung dieser Technologie in Russland, wo sie u. a zum Schutz von führenden Finanzinstituten, Handelsvertretungen, Behörden und Online-Shops eingesetzt wird, umfangreiche Erfahrungen sammeln können.