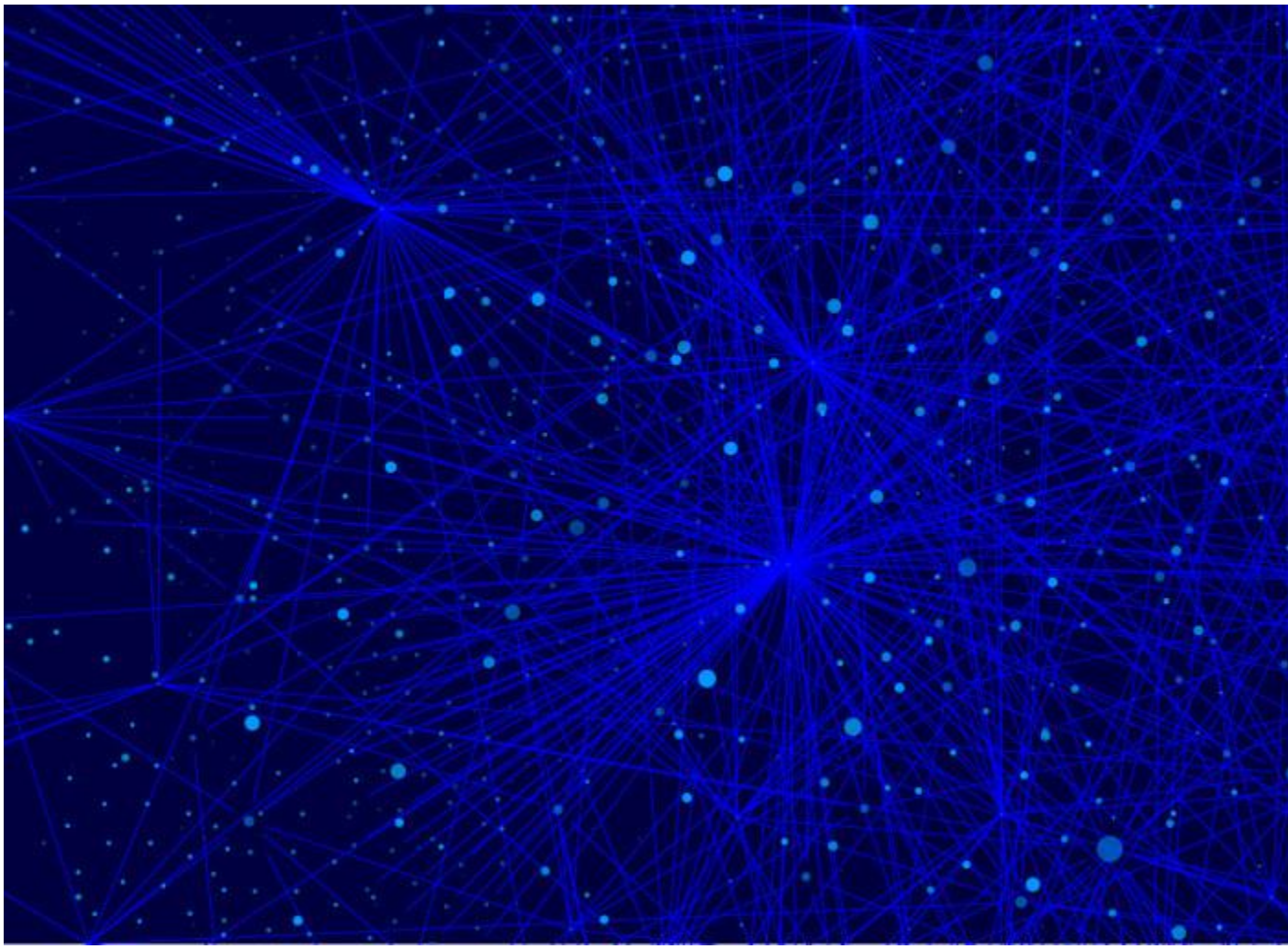
- AUTOR:. KIM ZETTERKIM ZETTER SICHERHEIT
- ERSCHEINUNGSDATUM: 01.16.16.01.16.16
- ZEITPUNKT DER VERÖFFENTLICHUNG: 7.00.7:00 UHR VORMITTAGS

HACKER LEXIKON: WAS SIND DOS- UND DDOS-ANGRIFFE?



Klicken Sie auf das Overlay-Galerie öffnen DANN ONE / WIRED

MAN SIEHT SIE in den Nachrichten die ganze Zeit erwähnt.DoS- und DDoS-Angriffe sind auf dem Vormarsch, und sie werden immer jedes Jahr anspruchsvoller und intensiver.Die US-Regierung beschuldigte den Iran, die Durchführung einer längeren Reihe von DDoS gegen die Web-Sites der Bank of America und andere Finanzinstitute, vermutlich als Vergeltung für Wirtschaftssanktionen gegen den Iran für sein Atomprogramm erhoben wird. Kürzlich DDoS-Attacken durch Erpresser haben Banken in Griechenland gezielte und Schweden. Also, was sind DoS und DDoS-Attacken?
DoS steht für "Denial of Service" und bezieht sich auf einen Angriff, der ein System mit überwältigt Daten am häufigsten eine Flut von gleichzeitigen Anforderungen an eine Website gesendet, um ihre Seiten zu sehen, was die Web-Server zum Absturz zu bringen oder einfach funktionsunfähig, da sie kämpft, um reagieren auf mehr Anfragen, als sie verarbeiten kann. Als Ergebnis sind legitime Benutzer, die die Website vom Server gesteuert zuzugreifen versuchen, nicht in der Lage, dies zu tun. Es gibt andere Arten von DoS-Attacken,die verschiedene Taktiken zu verwenden, aber sie alle haben die gleiche Wirkung: verhindert berechtigten Benutzern den Zugriff auf ein System oder eine Website.

TL; DR: Ein DoS oder Denial-of-Service-Angriff, flutet ein System, oft einen Web-Server, mit Daten, um sie zu überwältigen und verhindern, dass Benutzer den Zugriff auf eine Website. DDoS bezieht sich auf eine Distributed-Denial-of-Service-Angriff, die von mehreren Systemen an verschiedenen Standorten über das Internet verteilt kommt.

Einfache DoS-Attacken, von einer einzigen Maschine durchgeführt wird, sind selten in diesen Tagen.Stattdessen habe sie von DDoS-Attacken, Denial-of-Service-Attacken, die aus mehreren Computern über das Internet verbreitet, manchmal Hunderte oder Tausende von Systemen sofort kommen verdrängt worden. Die angreifenden Maschinen sind in der Regel nicht die Einleitung des Angriffs auf ihre eigenen, aber gefährdet sind Maschinen, die Teil eines Botnetzes von Hackern, die die Maschinen zu verwenden als eine Armee, um eine Website oder ein Zielsystem gesteuert werden. Da diese Angriffe gehen von Tausenden von Maschinen auf einmal, sie schwieriger zu bekämpfen sein können, indem Sie einfach blockieren den Verkehr von Maschinen, vor allem, wenn die Angreifer zu schmieden die IP-Adresse des angreifenden Computer, so dass es schwierig für die Verteidiger, um Verkehr zu filtern, basierend auf IP-Adressen.

Täter starten DDoS-Attacken für eine Vielzahl von Gründen.Hacktivisten habe sie verwendet werden, um Unmut gegen Ziele, zum Beispiel zum Ausdruck bringen, wenn Mitglieder der Anonymous startete Angriffe auf den Seiten von PayPal, Visa, Mastercard und im Jahr 2011 nach der Zahlungsdienstleister sich geweigert, finanzielle Spenden für Wikileaks soll verarbeiten.
Im Jahr 2013 startete offensichtlich Spammer eineBestrafung Angriff gegen die Spam-Bekämpfungs WebsiteSpamhaus, nachdem die Website hat ein Dutch-Hosting-Firma namens Cyberbunker seine Spam-Blacklist. Spamhaus bietet Blacklists, um E-Mail-Anbietern zu helfen, sie herausfiltern Spam von bekannten Spammern gesendet.Cyberbunker stand auf der Liste, weil es der Bereitstellung von Hosting-Services an Spammer angeklagt. Bei dem Angriff der Spitze, 75 Gigabit Datenverkehr pro Sekundeangeblich überschwemmt Spamhaus-Servern.
Die Online-Gaming-Industrie hat auch mit DDoS-Attacken seit mehreren Jahren geplagt, mit die Schuld werde verärgerten Spielern und sogar an Wettbewerber. Eine Reihe von DDoS-for-hire Dienstleistungen, für die Beispiele wird für jedes Unternehmen, das sie mieten will take down Website eines Konkurrenten.

Einige DDoS-Attacken sind für politische Zwecke ins Leben gerufen. Der berühmteste von ihnen waren die DDoS-Attacken, die Estland und Georgien ausgerichtet. Im Jahr 2007, eine Flut von Verkehrs klopfte Regierung und Medien-Websites in Estland offline und wurde später in russische Nationalisten, die wütend über Estland die Entscheidung waren zugeschrieben eine sowjetische Kriegsdenkmal verlagern in Tallinn vom Zentrum der Stadt auf einen Militärfriedhof.
Im Jahr 2008 wurden Web-Sites in Georgien mit DDoS-Attacken getroffen Wochen vor russischen Truppen in Südossetien und fordert Georgien und anderen an Russland für die digitalen Angriffen schuld.
In jüngerer Zeit haben DDoS-Attacken als kriminelle Erpressung Technik verwendet worden. Mehrere verschlüsselte E-Mail-Anbieter wie Protonmail und Hushmail sowie Banken in Schweden und Griechenland, haben mit DDoS-Attacken nach einem Rückgang um ein "Lösegeld" zu zahlen getroffen worden, um die Angreifer nicht Angriff ihre Websites gefordert hatte.
DDoS-Attacken können auch als Vorwand benutzt, um zu tarnen oder lenken die Aufmerksamkeit weg von anderen ruchlosen Aktivitäten ein Angreifer tun könnte, wie zum Beispiel Diebstahl von Daten von Netzwerk des Opfers werden. Hacker, die in Großbritannien Telekom Talktalk im vergangenen Jahr gezielt verwendet eine DDoS-Attacke alsVorwand, während sie auf 4 Millionen Kunden des Unternehmens abgeschöpft Daten.
DDoS-Angriffe sind nicht auf Computer und Web-Server beschränkt. Eine Variante des Angriffs können auch Telefone und Telefonanlagen abzielen. Im Dezember, als Hacker verursacht einen Stromausfall in zwei Werken in der Ukraine, sie leitete auch eine Telefonie-Denial-of-Service-Attacke gegen Kunden Call-Centern, für die Anwohner von der Berichterstattung den Ausfall an die Unternehmen zu verhindern.
DDoS-Attacken haben sich im Laufe der Zeit stärker, mit variierenden Hacker ihre Techniken, um ihre Wirkung zu verstärken und sie schwieriger zu mildern oder zu vereiteln.Jedes Jahr scheint es, zeigt eine neue Mega-DDoS-Attacke up, dass diejenigen, die ihr voraus Zwerge.

Letztes Jahr hat die San Francisco ansässigen Sicherheitsfirma CloudFlare, die hilft, Websites, ihre Leistung zu verbessern und die Sicherheit teilweise durch Milderung DDoS-Attacken, sagte, dass es einen massiven DDoS-Attacke gegen einen nicht identifizierten Kunden in Europa gekämpft hatte. Der Angriff, auf ihrem Höhepunkt,spuckte fast 400 Gigabit Daten pro Sekunde an seinem Ziel.Die durchschnittliche DDoS-Angriff ist etwa 50 Gbps.
Obwohl die Leistung von DDoS-Attacken nimmt zu, die Medien mischaracterize sie oft und zu übertreiben ihre Bedeutung. Viele Nachrichtenagenturen, zum Beispiel, haben irrtümlich auf die Vorlage Angriffe gegen Webseiten Estlands im Jahr 2007 als Cyberkriegsführung (unter ihnen, ein Magazin Wired Artikel). Und in einem 2012 Bloomberg Geschichte beschreibt, DDoS-Attacken gegen US-Banken, schrieb das Nachrichtenmagazin, dass "die Übergriffe hatten verstoßen einige der landesweit am weitesten fortgeschrittenen Computer Verteidigung", und dass

solche Angriffe Rang "unter den Worst-Case-Szenarien von der National Security Agency vorgestellt . "
In Wahrheit, DDoS-Angriffe allein sind ein Ärgernis Surfer und kostet ein Unternehmen entgangene Geschäfte während der Zeit, die sie Zugang zu Kunden zu verweigern, aber sie sind ziemlich einfach, gegen zu verteidigen. Bei der Verwendung in Verbindung mit einer Datenschutzverletzung oder einem anderen ruchlosen Aktivitäten können sie sicherlich an den Erfolg, den Verstoß zu unterstützen, aber kaum als katastrophal oder ein Worst-Case-Szenario zu qualifizieren unter niemandes Definition des Begriffs.

Zurück zum Anfang.Direkt zu: Start des Artikels.

- DDOS-
- HACKER-LEXIKON
- HACKS UND CRACKS