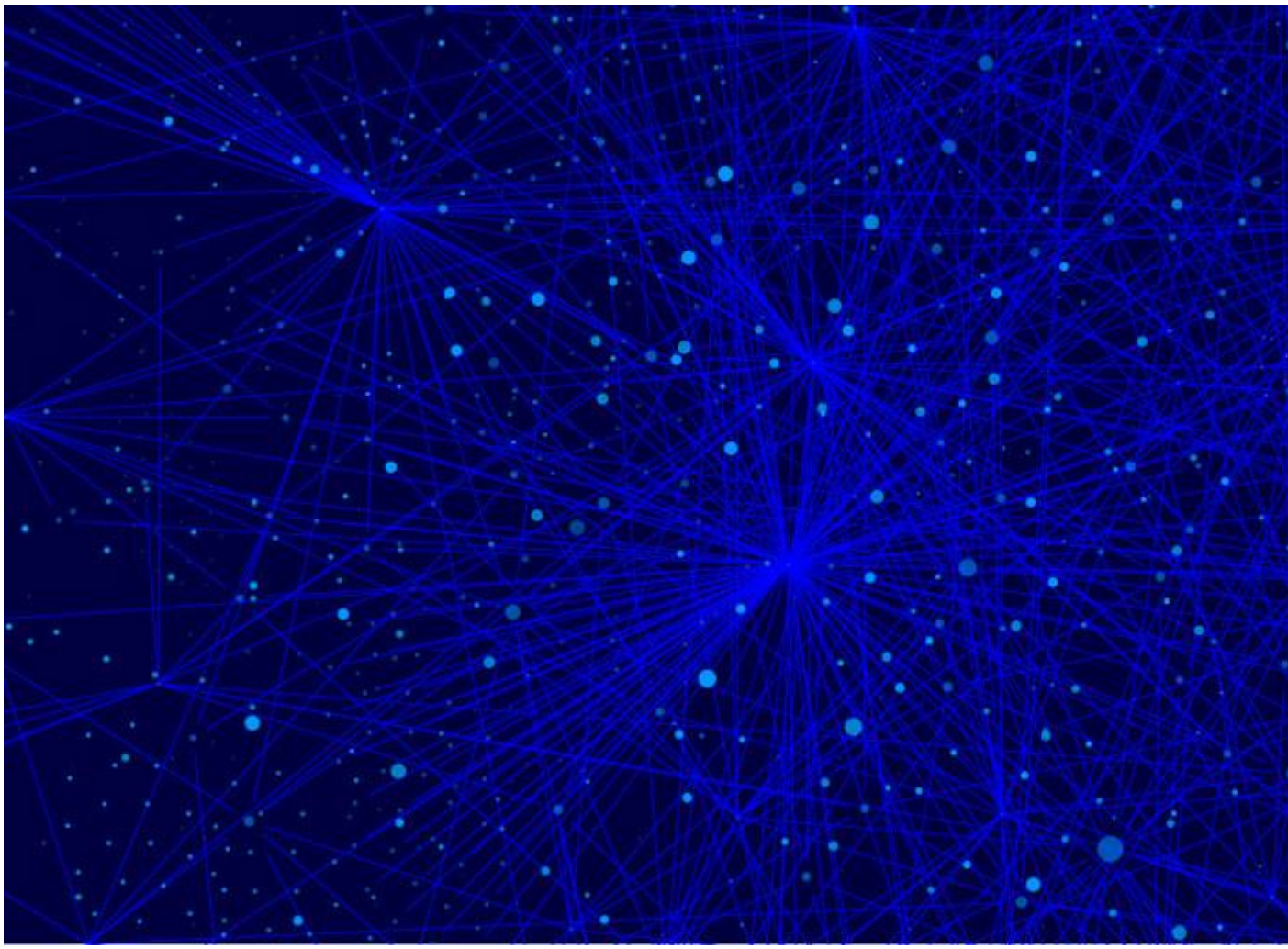
- Author: Kim Zetter. Kim Zetter Security
- Date of Publication: 01.16.16. 01.16.16
- Time of Publication: 7:00 am. 7:00 am

Hacker Lexicon: What Are DoS and DDoS Attacks?



Click to Open Overlay Gallery Then One/WIRED

You see them mentioned in the news all the time. DoS and DDoS attacks are on the rise, and they are getting more sophisticated and intense every year. The US government accused Iran of conducting a prolonged series of DDoS against the web sites of Bank of America and other financial institutions, presumably as retaliation for economic sanctions levied against Iran for its nuclear program. Recently DDoS attacks by extortionists have targeted banks in Greece and Sweden. So what are DoS and DDoS attacks?

DoS stands for "denial of service" and refers to an attack that overwhelms a system with data—most commonly a flood of simultaneous requests sent to a website to view its pages, causing the web server to crash or simply become inoperable as it struggles to respond to more requests than it can handle. As a result, legitimate users who try to access the web site controlled by the server are unable to do so. There are other types of DoS attacks that use

different tactics, but they all have the same effect: preventing legitimate users from accessing a system or site.

Simple DoS attacks, performed from a single machine, are uncommon these days. Instead, they've been supplanted by DDoS attacks, distributed denial-of-service attacks that come from many computers distributed across the internet, sometimes hundreds or thousands of systems at once. The attacking machines are generally not initiating the assault on their own but are compromised machines that are part of a botnet controlled by hackers who use the machines as an army to target a website or system. Because these attacks emanate from thousands of machines at once, they can be difficult to combat by simply blocking traffic from machines, especially when attackers forge the IP address of attacking computers, making it difficult for defenders to filter traffic based on IP addresses.

Perpetrators launch DDoS attacks for a variety of reasons. Hacktivists have used them to express displeasure against targets—for example when members of Anonymous launched attacks against the sites of PayPal, Visa, and MasterCard in 2011 after the payment service providers refused to process financial donations intended for WikiLeaks.

In 2013, spammers apparently launched a punishing attack against the spam-fighting site Spamhaus, after the site added a Dutch hosting company called Cyberbunker to its spam blacklist. Spamhaus provides blacklists to email providers to help them filter out spam sent from known spammers. Cyberbunker got on the list because it was accused of providing hosting services to spammers. At the attack's peak, 75 gigabits of traffic per second reportedly flooded Spamhaus servers.

The online gaming industry has also been plagued with DDoS attacks for several years, with the blame going to disgruntled players and even to competitors. A number of DDoS-for-hire services, for examples, will take down a competitor's website for any business that wants to hire them.

Some DDoS attacks are launched for political purposes. The most famous of these were the DDoS attacks that targeted Estonia and Georgia. In 2007, a barrage of traffic knocked government and media sites in Estonia offline and was later attributed to Russian nationalists who were angry about Estonia's decision to relocate a Soviet war monument in Tallinn from the center of the city to a military cemetery.

In 2008, web sites in Georgia were hit with DDoS attacks weeks before Russian troops invaded South Ossetia, prompting Georgia and others to blame Russia for the digital attacks.

More recently, DDoS attacks have been used as a criminal extortion technique. Several encrypted email providers like ProtonMail and Hushmail, as well as banks in Sweden and Greece, have been struck with DDoS attacks after declining to pay a "ransom" the attackers had demanded to not assault their web sites.

DDoS attacks can also be used as a smokescreen to camouflage or draw attention away from other nefarious activity an attacker might be doing, such as stealing data from the victim's network. Hackers who targeted the UK telecom TalkTalk last year used a DDoS attack as a smokescreen while they siphoned data on 4 million of the company's customers.

DDoS attacks are not limited to computers and web servers, however. A variation of the attack can also target phones and phone systems. In December, when hackers caused a power outage at two plants in Ukraine, they also launched a telephony denial-of-service attack against customer call centers, to prevent local residents from reporting the outage to the companies.

DDoS attacks have become more powerful over time, with hackers varying their techniques to amplify their effects and make them more difficult to mitigate or thwart. Every year it seems, a new mega-DDoS attack shows up that dwarfs those that preceded it.

Last year the San Francisco-based security firm CloudFlare, which helps sites improve their performance and security in part by mitigating DDoS attacks, said it had battled a massive DDoS attack against an unidentified client in Europe. The attack, at its peak, spewed nearly 400 gigabits of data per second at its target. The average DDoS attack is about 50 gbps.

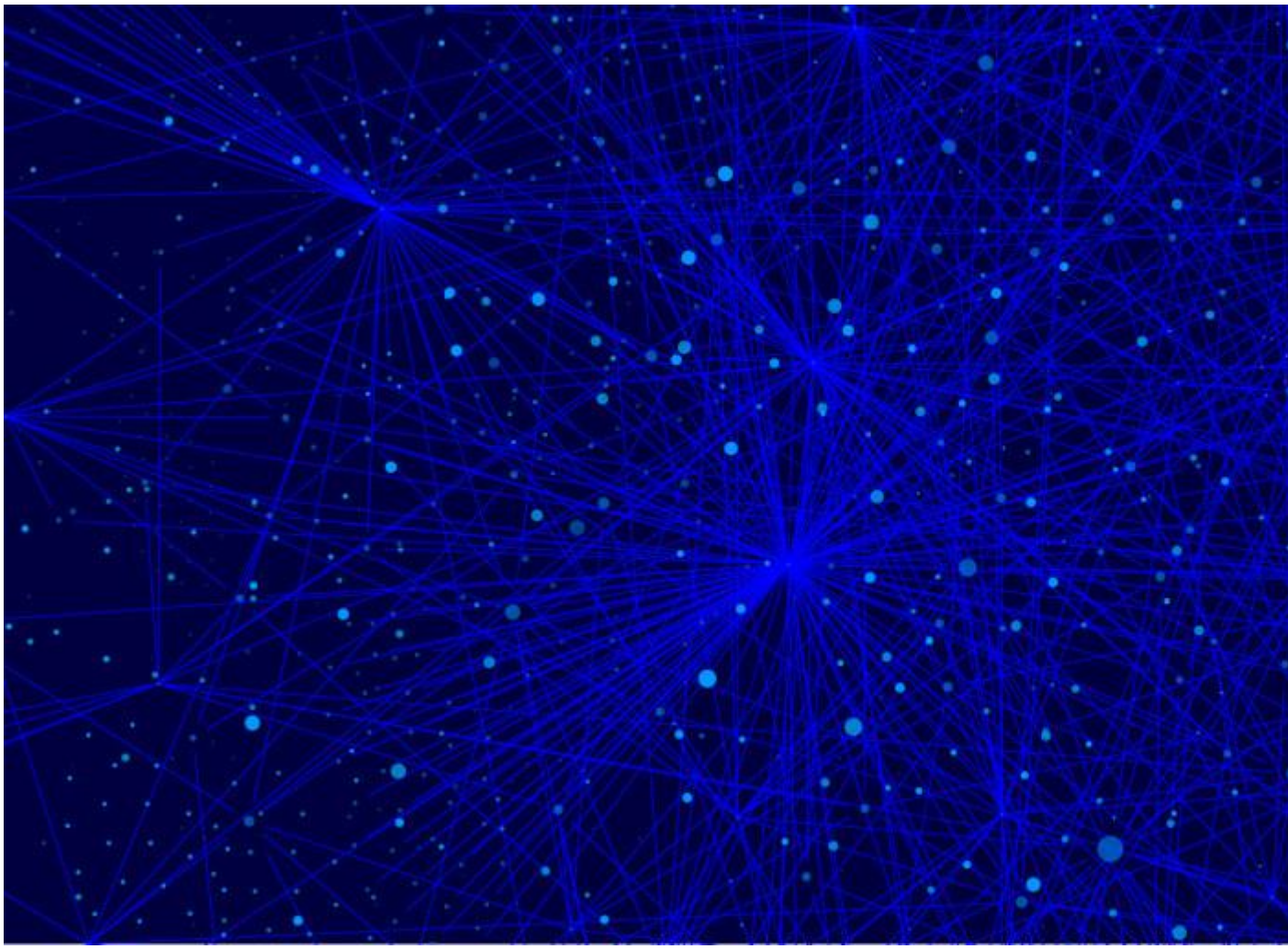
Though the power of DDoS attacks is growing, the media often mischaracterize them and exaggerate their significance. Many news outlets, for example, have erroneously referred to the attacks against Estonia's websites in 2007 as cyberwarfare (among them, a WIRED magazine article). And in a 2012 Bloomberg story describing DDoS attacks against US banks, the news outlet wrote that the assaults had "breached some of the nation's most advanced computer defenses" and that such attacks rank "among the worse-case scenarios envisioned by the National Security Agency."

In truth, DDoS attacks alone are an annoyance to web users and can cost a company lost business during the time they deny access to customers, but they're fairly easy to defend against. When used in conjunction with a data breach or some other nefarious activity they can certainly assist in the success of that breach, but they hardly qualify as catastrophic or a worst-case scenario under anyone's definition of the term.

http://www.wired.com/2016/01/hacker-lexicon-what-are-dos-and-ddos-attacks/

- 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-AN-GRIFFE?



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