Stürmische See

DDoS-Angriffe werden zur Gefahr für das Internet

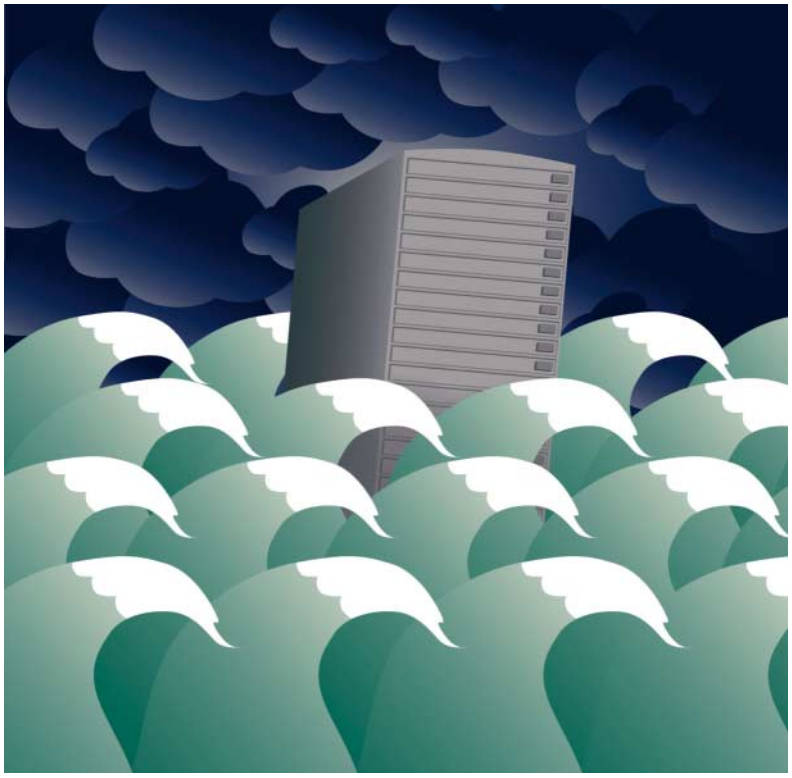


Bild: Bettina Keim

Lange waren DDoS-Angriffe lediglich eine lästige Störung, die Betreiber von Webseiten meistens aussitzen konnten. Diese Zeiten scheinen vorbei zu sein. Die Angriffe werden immer häufiger, immer heftiger und es ist abzusehen, dass Staaten in zukünftigen Konflikten ganze Teile des Internet ausschalten.

Von Fabian A. Scherschel

Anfangs waren sie nur eine kleine Nische für wenige, spezialisierte Kriminelle. Jetzt sind sie allgegenwärtig und treffen hierzulande verstärkt mittelständische Unternehmen: Distributed-Denial-of-Service-Angriffe (DDoS). Firmen, für die jede Sekunde ohne funktionierende Webseite verlorenes Geld ist, werden zum Ziel spezialisierter Banden, die mit Botnetzen bewaffnet ihren Opfern die Pistole auf die Brust setzen – Geld her oder eure Webseite ist für Tage nicht erreichbar! Seit im kriminellen Untergrund Dienste auf den Plan getreten sind, über die man DDoS-Angriffe bequem per Web-Interface bucht, kann jeder mitmachen, der genügend Willen und kriminelle Energie besitzt. Die vereinfachte Verfügbarkeit von DDoS-Angriffen hat auch die Hemmschwelle der Angreifer gesenkt.

DDoS-Dienste sind ähnlich wie die Malware-Industrie arbeitsteilig organisiert: Botnet-Betreiber vermieten ihre Netze an Zwischenhändler, die über Web-Frontends die Angriffs-Aufträge der zahlenden Kunden entgegennehmen. Die meisten Angreifer versuchen, Geld durch Erpressung von Bitcoins zu verdienen. Aber mittlerweile werden DDoS-Angriffe oft auch durchgeführt, um unliebsame Meinungen zu unterdrücken – ganz egal, ob es sich dabei um politische Aussagen, aktuelle personenbezogene Berichterstattung oder einfach nur eine andere Meinung zu einem Videospiel handelt.

Die See wird rauer

Blizzard Entertainment wurde mit der Veröffentlichung einer neuen World-of-Warcraft-Erweiterung vor Kurzem erst wieder Opfer langanhaltender Angriffe – höchstwahrscheinlich deshalb, weil einigen Spielern die Änderungen nicht gefielen. Der unabhängige Journalist Brian Krebs machte Schlagzeilen mit einer massiven DDoS-Attacke auf seine Webseite. Krebs recherchiert im kriminellen Untergrund und hat sich so bei Drogendealern ebenso unbeliebt gemacht wie bei Kreditkarten-Betrügern. Ein Dealer hatte ihm sogar schon einmal Heroin geschickt, um ihn bei der Polizei anzuschwärzen. Nach seinen Berichten über die Festnahme der israelischen Betreiber des DDoS-Dienstes vDoS geriet allerdings sein Blog in den Fokus der Angreifer.

Der Angriff, den diese als Rache für seine Artikel lostraten, war so mächtig, dass selbst Akamai, einer der größten Anbieter auf dem Gebiet der DDoS-Abwehr, klein beigeben musste. Akamai hatte die Webseite von Krebs gratis geschützt und dieses Arrangement angesichts der überwältigenden Traffic-Fluten, die auf die Server von Krebs einbrachen, gekündigt. In der Spitze erreichte der Angriff bis zu 620 Gigabit pro Sekunde. Bemerkenswert war hierbei nicht nur die schiere Masse des bösartigen Traffics – fast doppelt so viel wie Akamai bisher je in einem DDoS-Angriff gesehen hatte –, sondern auch die Tatsache, dass dieser Angriff gänzlich ohne Reflection-Methoden auskam. Über Reflection benutzen die Angreifer die sehr gute Anbindung großer Server, um ihre Angriffe zu verstärken. Das heißt, beim Angriff auf Krebs muss ein enormes Botnetz im Spiel gewesen sein – ein Botnetz, das bisher nicht in Erscheinung getreten war. Und es heißt auch, dass sie das Potenzial ihrer Zombie-Rechner noch enorm erhöhen können, wenn sie zusätzliche Reflection-Tricks verwenden.

Angriffe dieses Ausmaßes klingen schon äußerst bedrohlich, wenn sie von Kriminellen durchgeführt werden. Aber auch staatliche und staatsnahe Organisationen geraten immer wieder in den Ver-

dacht, DDoS-Angriffe auszuführen. Im Arsenal des sogenannten Cyberkriegs bilden sie so etwas wie die Artillerie des konventionellen Militärs: Mit ihnen sollen Ziele abgelenkt und mürbe gemacht werden, damit Einsatztruppen aus Hackerteams einfacher in die Zielsysteme eindringen können.

DDoS-Attacken eignen sich auch dazu, den politischen Gegner zu provozieren. Ihre Herkunft lässt sich besser verschleiern als die meisten anderen Hacker-Angriffe. Oft stammen die Traffic-Fluten von Botnetzen, die aus den zu Zombies verwandelten Rechnern ahnungsloser Privatpersonen zusammengestrickt sind. Zwar lässt sich der Traffic unter Umständen auf einzelne IP-Adressen zurückführen. Nachdem aber fast der ganze DDoS-Verkehr von den infizierten Rechnern ansonsten Unbeteiligter stammt, versandet die Spur der Ermittler an dieser Stelle. Die Systeme mögen in Russland, Thailand, China oder Castrop-Rauxel stehen: Wer sie gehackt oder die gehackten Rechner für einen Angriff gekauft hat, lässt sich nur selten zurückverfolgen. Und da das Internet der Dinge dafür sorgt, dass jeden Tag mehr Computer an immer überraschenderen Orten installiert werden – oft mit wenig oder gar keinem Gedanken an deren Absicherung. Die Anzahl von Zombie-Rechnern und damit die Bandbreite von DDoS-Angriffen wird auf absehbare Zeit nur weiter zunehmen.

DDoS gegen das ganze Netz

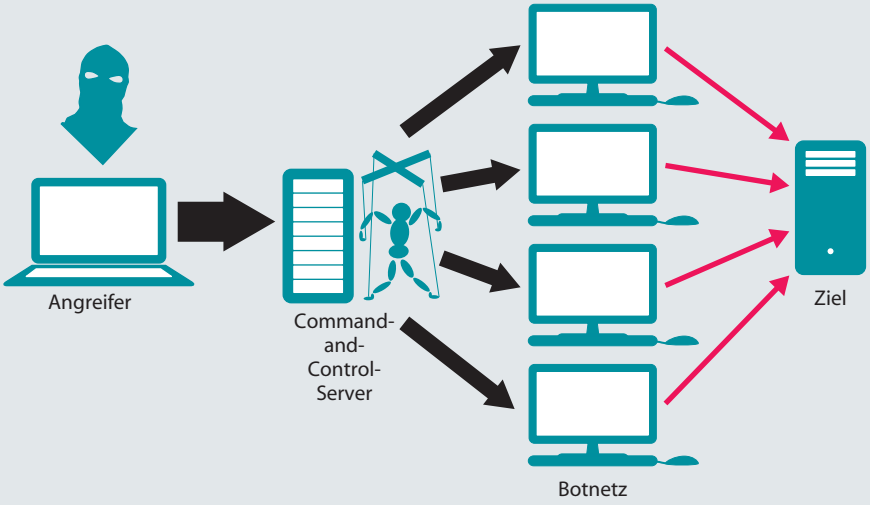
Bisher waren DDoS-Angriffe für Staaten vor allem interessant, weil sie so den Institutionen ihrer Kontrahenten schaden können, ohne Angst vor Repressionen haben zu müssen. Das gezielte Eindringen in fremde Netze hat weitreichendere Folgen, wie beim Einbruch in das Parlamentsnetz des Bundestages im vergangenen Jahr oder dem Hack des Democratic National Committee im US-Wahlkampf zu beobachten war. Solche Hacks sind aber auch mit größeren Risiken verbunden als DDoS-Angriffe. Neuerdings beobachten Firmen, die mit der Bekämpfung von DDoS-Attacken ihr Geld verdienen, dass sich die Rolle dieser Angriffe ändert. Es scheint so, als wolle man nicht nur noch den Gegner ablenken oder Verwirrung stiften (wie zum Beispiel beim Ausbruch der Ukraine-Krise), sondern die DDoS-Artillerie auch als Waffe gegen ganze Teile des Internet aufrüsten.

Sicherheitsfirmen haben in den letzten Monaten verstärkt Angriffe beobachtet, die aussehen, als ob sie die Verteidigungsmöglichkeiten ihrer Ziele genau ausloten. Ein Angriff beginnt mit einer gewissen Menge an Traffic und fährt die Intensität des Bombardements dann allmählich immer weiter nach oben, bis der Angriff auf einmal aufhört. Tage später geht es dann auf genau diesem Level weiter und die Menge des Traffics wird wieder langsam erhöht. Außerdem haben die Angriffe gemeinsam, dass viele DDoS-Methoden zum Einsatz kommen. Das Ganze sieht aus, als wolle jemand den genauen Punkt herausfinden, ab dem die Verteidiger aufgeben müssen und das entsprechende Ziel überwältigt ist.

Der renommierte Sicherheitsexperte Bruce Schneier, mittlerweile Cheftechnologe bei einer IBM-Tochter, die sich mit der Abwehr von Hackerangriffen befasst, machte als einer der ersten öffentlich auf diese Vorkommnisse aufmerksam.

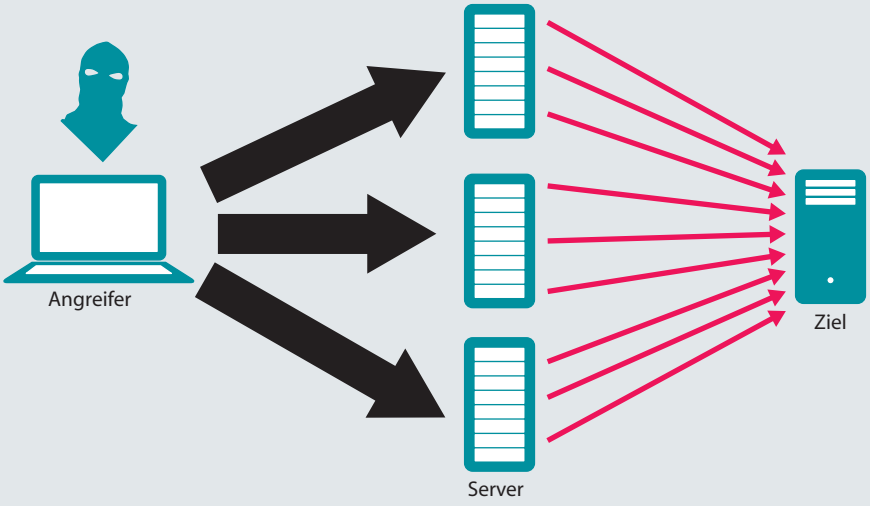
Botnetz-Attacke

Mit Hilfe eines Botnetzes aus gekaperten Rechnern überlastet der Angreifer den Zielserver. Die Bots werden über denCommand-and-Control-Server mit Befehlen versorgt. Mittlerweile können Dritte solche Botnetze bequem über ein Web-Interface mieten.



Reflection-Angriff

Unter Reflection versteht man, wenn der Angreifer sich die gute Netzanbindung unbeteiligter Drittserver zunutze macht, um das Ziel anzugreifen. Er schickt einzelne Datenpakete an die Server, die wiederum eine Vielzahl an Traffic generieren, der auf das Angriffsziel gerichtet ist.



Schneier hält die Angriffe für Testläufe. Seiner Meinung nach schießt sich ein Staat oder eine staatsnahe Organisation darauf ein, in Zukunft große Teile des Internet lahmlegen zu können. Schneier fühlt sich an Militärtaktiken aus dem Kalten Krieg erinnert, als die Konfliktparteien immer wieder methodisch in den Luftraum des Gegners eindrangen, um dessen Flugabwehrsysteme zur Reaktion zu zwingen – auf diese Art ließen sich deren Fähigkeiten und Schwächen beobachten.

Die Geschichte von der DDoS-Superwaffe ist momentan noch Spekulation. Sicher ist allerdings, dass DDoS-Angiffe immer häufiger und immer mächtiger werden. Verisign, als Registrar der wichtigen Domains .com, .gov und .net ein ständiges Ziel für DDoS-Angriffe, hat bis Mitte dieses Jahres 75 Prozent mehr DDoS-Angriffe festgestellt als in derselben Zeit im Jahr davor. Knapp ein Drittel dieser Angriffe fand mit mehr als 10 Gigabit pro Sekunde statt.

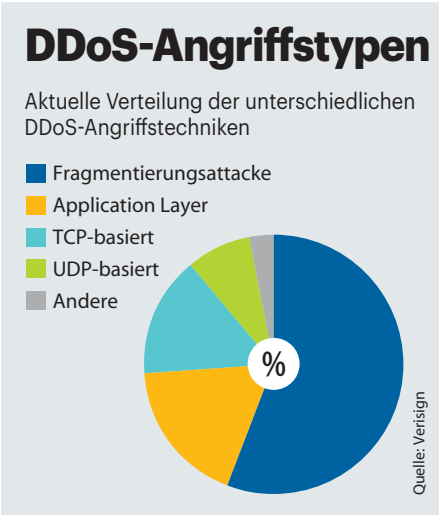
Nach den Erkenntnissen der Anti-DDoS-Sparte der Firma stieg das Angriffsvolumen Anfang des Jahres 2016 rasant an – den Angreifern stehen augenscheinlich immer mehr kompromittierte Rechner zur Verfügung, um Angriffe auszuführen. Und das Ausloten des Gegners, wie Schneier es im großen Stil beschreibt, kommt schon bei kleineren Angriffen von DDoS-Erpressern zum Tragen. Das alles führt dazu, dass es immer schwieriger wird, sich gegen DDoS-Attacken zu wehren.

Angriffe auf c't und heise online

Systematische Angriffe, bei denen nicht eine, sondern mehrere DDoS-Methoden zum Einsatz kommen, werden immer häufiger. Das deutet auf besser organisierte und professionelle Angreifer hin. Auch beim Angriff auf die Webseiten von c't und heise online im Mai wegen eines unliebsamen Artikels konnten wir beobachten, wie die Angreifer zuerst eine Angriffsmethode einsetzten und dann auf eine andere umstiegen, nachdem unsere Admins den ersten Angriff abgewehrt hatten. Wie wir nun herausfanden, hatte der Angreifer den DDoS-Dienst vDoS benutzt, über den auch Brian Krebs berichtet hatte. Im Internet veröffentlichte Logdateien nach einem Hack der vDoS-Systeme zeigen, wie der Angreifer zuerst eine SYN Flood beantragt hatte und später auf Amplification-Angriffe per DNS und NTP umstieg.

Zwar wurden die Betreiber von vDoS mittlerweile verhaftet; Experten der Anti-DDoS-Dienste erwarten dadurch allerdings keinen langfristig nennenswerten Rückgang der Angriffswellen. Ein Vertreter von Akamai sagte im Gespräch mit c't dazu, dass das Gesamtvolumen der Angriffe einfach zu groß sei, als dass der Wegfall eines einzigen solchen DDoS-Dienstes ins Gewicht fallen würde. Wie bei Malware-Schreibern und Untergrund-Marktplätzen führt die Verhaftung einer Gruppe von Ganoven in der Regel dazu, dass ihre Nische schnell von Konkurrenten gefüllt wird.

Zum Schutz vor DDoS-Angriffen können sich Kunden entweder unter den Schirm von spezialisierten Anbietern wie Akamai, Cloudflare oder Link 11 begeben, oder sich die zur Abwehr nötige Hardware ins eigene Rechenzentrum stellen. Letzteres kann aber schnell ins Geld gehen: Um beispielsweise verlässlich Angriffe von bis zu 500 Megabit pro Sekunde wegschaufeln zu können, ist Hardware für gut 50.000 Euro nötig. Außerdem hilft das nichts, wenn der Angreifer stark genug ist, die Anbindung des Providers lahmzulegen. Von daher dürfte für die meisten Kunden ein Anti-DDoS-Anbieter die bessere Wahl sein. Ob einen die Anbieter auch noch schützen können, wenn man sich wie Brian Krebs mit einem mächtigen Gegner anlegt, steht auf einem anderen Blatt. *(fab@ct.de)* c't



Was ist ein DDoS-Angriff?

Das Ziel eines Denial-of-Service-Angriffs ist es, den Zielserver lahmzulegen. Das führt dazu, dass legitime Anfragen von normalen Webseiten-Besuchern in der Flut des Angriff-Traffics untergehen – für den Besucher sieht es so aus, als ob die Webseite nur sehr langsam oder gar nicht lädt. Wird der Server komplett lahmgelegt, ist er für niemanden mehr zu erreichen.

Da die Mengen an Traffic, die benötigt werden, um moderne Server aus dem Internet zu spülen, nicht mit einem System zu erzeugen sind, braucht der Angreifer mehrere Ausgangsrechner. Nun spricht man von einem Distributed Denial of Service, da der Angriff von vielen verteilten Systemen ausgeführt wird. Diese können sich an unterschiedlichen Enden der Welt befinden und werden meist als sogenanntes Botnetz von Kontrollservern auf das jeweilige Ziel ausgerichtet.

Gegen solche Angriffe kann man sich grundsätzlich auf zwei Arten verteidigen. Erstens kann man die maximale Bandbreite des eigenen Servers erhöhen und den bösartigen Traffic einfach aushalten, während man die echten Anfragen beantwortet. Zweitens kann man zusätzlich versuchen, so viel wie möglich des DDoS-Traffics zu blocken. Da aber auch das Filtern an sich Resourcen verbraucht, funktioniert das nur bis zu einem gewissen Punkt. Das perfide an einem raffiniert ausgeführten DDoS-Angriff ist, dass der Verteidiger den bösartigen Traffic nur schwer von legitimen Besuchern seiner Webseite unterscheiden kann. Bei Reflection-Angriffen kommt erschwerend hinzu, dass der Angreifer legitime Server im Netz dazu bringt, den eigenen Angriff um ein Vielfaches zu verstärken.

Selbst wenn man es schafft, die eigene Infrastruktur so auszulegen, dass sie den Angriff aushält, hat man immer noch das Problem, dass die vorgelagerten Systeme – zum Beispiel der Service Provider – den Angriff nicht aushalten. Um sich effektiv gegen DDoS-Attacken abzusichern, muss man also zwangsläufig mit den Parteien zusammenarbeiten, welche für die Anbindung der Server an das öffentliche Netz verantwortlich sind. Deshalb lenken große Anti-DDoS-Anbieter den Traffic ihrer Kunden möglichst früh in eigene Netze, die entsprechend proportioniert sind.