Der Spamhaus/CloudFlare/Stophaus Denial of Service Angriff

8. 4. 2013

Zusammenfassung

In der zweiten Märzhälfte 2013 kam es zu einer Serie von heftigen Denial-of-Service Angriffen auf „Spamhaus“, einem Anbieter von Anti-Spam Blocklisten. In manchen Medien wurde dieser als Gefahr für die Stabilität des Internets beschrieben.

Das war weit übertrieben: weder war die Angriffsmethode neu, noch war die Angriffsstärke um Größenordnungen höher als das bisher gesehene. Die Kollateralschäden für unbeteiligte Dritte blieben auf wenige Punkte im Netz beschränkt: die überwiegende Mehrheit der Internet-Nutzer blieb von dem Ereignis völlig unberührt.

Sowohl die Angreifer als auch die Verteidiger haben während des Angriffs ihre Strategien flexibel an die Reaktion des Gegners angepasst, letztlich war aber die gut eingespielte Kooperation der Betriebsführungsteams der Netzbetreiber erfolgreich und diese konnten die Attacken gemeinsam abwehren. CERT.at als das österreichische nationale CERT ist in diese globale Zusammenarbeit eingebunden.

Dennoch hat der Angriff einige Probleme aufgedeckt, die behoben werden sollten:

- Fehler in der Absicherung der Internet-Basisinfrastruktur (Filter in Routing-Protokollen, Control-Plane Protection, …)
- Mangelnder Schutz gegen das Einspeisen von gefälschten IP-Paketen
- Fehlkonfiguration bei Nameservern, die sich dadurch als Angriffs-Verstärker ausnutzen lassen

Autor:

Otmar Lendl <lendl@cert.at>

Feedback:

Kommentare oder Rückfragen bitte an team@cert.at.

Inhalt

Hintergrund

Schon bald nachdem Spam (unerwünschte Werbung per Email) in den Neunzigerjahren zu einem ernsten Problem geworden ist, entstanden diverse Online-Datenbanken, die auch heute noch zum Blockieren der IP-Adressen der Spamsender herangezogen werden. Siehe Wikipedia[1] für eine Definition und einen historischen Überblick zu diesen „Real-time blackhole list (RBL)“ oder „DNS-based Blackhole List (DNSBL)“.

Die Betreiber dieser RBLs variieren von Einzelpersonen über lose Zusammenschlüsse bis hin zu kommerziellen Organisationen. Es existieren viele dieser Listen[2] im Internet, die alle leicht unterschiedliche Kriterien und Quellen zur Aufnahme benutzen. Siehe etwa http://multirbl.valli.org/ für ein Interface, um viele dieser RBLs auf einmal anzufragen.

Wird eine RBL von vielen Mailserverbetreibern als Ausschließungsgrund für eingehende Email herangezogen, dann hat der Betreiber der RBL einen signifikanten Einfluss auf die Fähigkeit einer IP-Adresse, global Email zu versenden. Das hat im Laufe der Zeit zu einigen juristischen Auseinandersetzungen zwischen den Listenbetreibern und den von diesen als Spammer – oder als „Spammerunterstützer“ – eingestuften Organisationen geführt.

„Spamhaus[3]“, eine europäische Firma (primär mit Sitz in der Schweiz und UK) betreibt mehrere RBLs, die private Mailserverbetreiber gratis nutzen dürfen, und von vielen Internet Service Providern (ISP) gegen Geld zur Spamfilterung herangezogen werden. Spamhaus ist umstritten, da es nicht nur IP-Adressen in seine Listen aufnimmt, die direkt aktiv zum Versenden von Emails benutzt werden, sondern versucht, die Spamversender komplett aus dem Netz zu drängen. Falls dazu die Beschwerden an die Provider der Spammer nicht ausreichen, listet Spamhaus immer größer werdende Adressbereiche rund um die eigentlichen Spamversender, um den Druck auf den ISP zu erhöhen. Dadurch entsteht Kollateralschaden bei den ISPs (von Spamhaus dann „Spam supporting services“ genannt), der diese dazu bringen soll, die Accounts (und andere Ressourcen) der Spammer einseitig zu kündigen.

Spamhaus ist einer jener Anti-Spam Kämpfer, die sehr fundamentalistisch eingestellt sind. Im Fokus ist Spam; dieser ist (laut Spamhaus) „böse“ und muss eliminiert werden. Alle anderen Gesichtspunkte haben sich diesem Ziel unterzuordnen. Es gab daher auch schon mehrere Zwiste zwischen Spamhaus und legitimen Organisationen, etwa den ccTLD Registries von Österreich und Lettland. Auch den Versuch, Spamhaus in der Person von Richard Cox in die RIPE Anti-Abuse Workinggroup[4] einzubinden, kann man als gescheitert ansehen[5].

Auf der anderen Seite existieren neben den echten „Cyber“-Kriminellen auch manche Dienstleister, die ihren Kunden nicht mittels der AGB ein Wohlverhalten im Netz vorschreiben wollen. Darunter finden sich Verfechter von Internet-Freiheit und radikalen Anti-Zensur Gruppierungen, die möglichst wenige Einschränkungen auf die Nutzung des Internets haben wollen. Die Palette reicht von Enthüllungsportalen wie WikiLeaks, über Portalen, die der Content-Industrie ein Dorn im Auge sind (Torrent Sites wie „Pirate Bay“, File Hoster, …) bis hin zum Hosten von Phishing-Backends oder

[1] https://en.wikipedia.org/wiki/DNSBL
[2] https://en.wikipedia.org/wiki/Comparison_of_DNS_blacklists
[3] http://www.spamhaus.org/
[4] https://www.ripe.net/ripe/groups/wg/anti-abuse
[5] http://www.ripe.net/ripe/groups/wg/anti-abuse/minutes/ripe-61

Exploit-Packs. In diesem Bereich findet man Aussagen wie „Wir hosten alles außer Kinderpornografie und Terroristen“[6]; jede der üblichen Netzmissbrauchsbeschwerden werden ignoriert oder mit dem Verweis auf die Polizei („Wir reagieren nur auf Gerichtsbeschlüsse, wir zensurieren unsere Kunden nicht“) beantwortet. Cyberbunker / CB3ROB ist ein Paradebeispiel für diese Gruppe. Siehe etwa das Portrait[7] von Sven Olaf Kamphuis von CB3ROB.

Im März 2013 kam es zu einem „Showdown“ zwischen diesen beiden extremen Standpunkten: Spamhaus hat die Upstream-Provider von Cyberbunker bedrängt, diesen vom Netz abzuhängen. Darauf kam es zu einem Zusammenschluss mehrerer Gruppen aus den fragwürdigen Ecken des Internets, die sich unter dem Namen „Stophaus“[8] gegen den Druck von Spamhaus wehren wollten.

Als Gegendruckmittel wurde ein BGP Hijacking und ein massiver Denial-Of-Service Angriff gegen Spamhaus gestartet.

Verlauf der Angriffe

BGP Hijacking

Am 21. März berichtet Greenhost[9], ein Webhoster in den Niederlanden, von einer Anomalie in den Erreichbarkeitsinformationen, die sein Router am NL-IX, einem Internet Exchange Point (IXP) gelernt hatte.

Die IXPs sind Austauschknoten für Internet-Verkehr: die angeschlossenen Router der Provider tauschen über das Border Gateway Protokol (BGP) Informationen über Erreichbarkeit von Netzblöcken (Routen) aus. Aufgrund der mittels BGP gelernten Routing-Informationen wissen die Router der ISPs, an welchen anderen Netzbetreiber sie ein bestimmtes IP-Paket weiterleiten sollen.

Auch schon im Februar 2008 kam es zu einem Vorfall[10], als Pakistan Telecom fälschlicherweise den Netzbereich von Youtube annonciert hat, was zu weitreichenden Störungen geführt hat.

Das aktuelle BGP-Hijacking (Ankündigen von fremden Netzen über BGP) war offensichtlich Absicht: Es wurde von CB3ROB die Route zu exakt einer IP-Adresse – der eines Nameservers von Spamhaus – injiziert, und dort war ein Nameserver so konfiguriert, dass die so abgezweigten Anfragen auch mit „das ist ein Spamsender“ beantwortet. Die Motivation dahinter war, die Nutzung der Spamhaus Blockliste zu stören.

Angriff gegen Spamhaus

Dass Spamhaus mit „Distributed Denial-of-Service (DDoS)”-Angriffen zu tun hat, ist nichts neues. Deren Position im Netz, verbunden mit den offensichtlichen Antagonisten, führte in der Vergangenheit schon öfters dazu. Daher sind vor allem die Nameserver von Spamhaus, über die die

[6] http://cyberbunker.com/web/stay-online-policy.php
[7] https://www.nytimes.com/2013/03/30/business/global/after-cyberattack-sven-olaf-kamphuis-is-at-heart-of-investigation.html?ref=technology&_r=0
[8] https://twitter.com/stophaus, http://stophaus.com/
[9] https://greenhost.nl/2013/03/21/spam-not-spam-tracking-hijacked-spamhaus-ip/
[10] https://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

DNSBL abgefragt wird, massiv redundant ausgeführt. Der aktuelle DDoS Angriff richtete sich gegen die Web-Präsenz von Spamhaus.

Bei einem DDoS Angriff werden so viele Anfragen an das Opfer gesendet, dass dieses oder seine Internet-Anbindung so überlastet wird, dass legitime Anfragen nicht mehr beantwortet werden können.

Wann der erste Angriff im März genau begonnen hat, ist uns nicht bekannt. Er scheint jedenfalls die Kapazitäten von Spamhaus dermaßen überlastet zu haben, dass Spamhaus am 19. März den bekannten Anbieter „CloudFlare[11]“ um Hilfe geben hat.

CloudFlare betreibt eine weltweit verteilte Infrastruktur, die als Content Delivery Network (CDN) für ihre Kunden agiert. Im Gegensatz zu den klassischen CDNs (etwa Akamai) ist der Fokus von CloudFlare weniger die Bereitstellung von oft angefragten Downloads, sondern das Abfangen von DoS-Angriffen. Die CloudFlare-Server arbeiten als Filter, die nur legitime Anfrage an den Webserver des Auftraggebers weiterleiten.

Die technischen Details hat CloudFlare in einem Blogbeitrag[12] ausführlich dokumentiert. Demnach war der Hauptteil des Angriffs ein Versuch, die Leitungen in Richtung des Opfers mit Datenmüll zu füllen. Aus technischer Sicht war das ein DNS-Amplification Attack. Dazu später mehr.

Angriff gegen CloudFlare

Die Anycasting-Infrastruktur von CloudFlare konnte die Wucht des Angriffs (bis zu 75 Gbit/s) gut auf alle Standorte verteilen und so beherrschbar machen.

Als Reaktion darauf stellten die Angreifer ihre Strategie um: Anstatt die bei CloudFlare gehosteten Webseiten von Spamhaus anzugreifen, gingen sie direkt auf die Infrastruktur der einzelnen CloudFlare-Standorte los. Das war von CloudFlare deutlich schwieriger abzuwehren, da der Vorteil der verteilten Infrastruktur nicht mehr gegeben war.

Eine der üblichen Abwehrmaßnahmen bei DDoS-Angriffen mit hohem Paketvolumen ist, die Störpakete möglichst früh herauszufiltern. Dazu bittet das Opfer seinen Internet Service Provider (ISP), den Angriff bereits auf seiner Seite zu blockieren, damit die Leitung vom ISP zum Opfer nicht mehr belastet wird.

Das hat auch hier funktioniert, und damit konnte der Angriff wieder bewältigt werden.

Angriff gegen die Netzwerkanbindung von CloudFlare

Als Reaktion darauf haben die Angreifer das Ziel erneut gewechselt, und die Infrastruktur der ISPs von CloudFlare attackiert. Da das Ziel nicht mehr greifbar war, wurden dessen Lieferanten attackiert, wohl in der Hoffnung, dass diese CloudFlare (und damit Spamhaus) fallen lassen (dass gerade das der von Stophaus kritisierte Modus Operandi von Spamhaus ist, entbehrt nicht einer gewissen Ironie).

In dieser Phase der Angriffe wurden dann 300 Gbit/s an Stördaten gemessen. Das ist zwar für aktuelle globale Internet-Backbones (Tier-1 Provider) kein unmittelbares Problem, dort sind Verkehrsströme im Terabit-Bereich üblich (siehe etwa die Statistiken vom DE-CIX, LINX oder AMS-IX).

[11] http://www.cloudflare.com/
[12] http://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho

Aber 300 Gibt/s zusätzlich auf nur einem Punkt im Netzwerk ist auch für diese Provider ein Problem, da einzelne Verbindungen aktuell nie mehr als 100 Gbit/s transportieren können und freie Kapazitäten in dieser Höhe nicht überall als Reserve vorgehalten werden können.

Neben der Anbindung an Tier-1 Provider ist CloudFlare auch (direkt und indirekt) über „Internet Exchange Points (IXPs)“ an den Rest des Internets angekoppelt. Auch ihre Infrastruktur wurde attackiert und es kam auch zu Beeinträchtigungen in der Anbindung von unbeteiligten Netzen.

Spätestens an diesem Punkt haben auch die zentralen Betreiber der des globalen Internets diese Angriffe aktiv bekämpft und in den Griff bekommen. Das Internet läuft nicht auf Autopilot, es wird überall aktiv von Menschen überwacht, nachjustiert und an aktuelle Vorfälle angepasst. Das mögen technische Störungen sein (etwa Fehler in einzelnen Komponenten), ausgefallene Leitungen (z.B. von Schiffsankern zerrissene Unterseekabel), sich ändernde Anforderungen (neue Kunden, anderes Nutzerverhalten, Verkehrswachstum, …) bis hin zu solchen DDoS Angriffen[13].

In diesem Fall wurden die 300 Gbit/s auch nicht an einem Punkt gemessen. Der Angriff war ein DDoS, also ein verteilter („distributed“) Denial-of-Service Attack: er wurde nicht von einem Punkt aus losgeschickt, sondern hat viele – im Netz weit verteilte – Sender und Verstärker benutzt. Indem man die Filter zur Abwehr auch weit im Netz verteilt installiert hat, wurden die Angriffswellen früh unterbunden und konnten sich nicht am Ziel treffen und dort zum großen Tsunami aufschaukeln.

Ende der Angriffe

Warum die Angriffe dann abgeflacht sind, ist nicht klar. Es gibt dazu mehrere Interpretationen:

- Das Ziel, Spamhaus aus dem Netz zu schießen, hat sich als nicht machbar erwiesen. Die Eskalation der Angriffe auf die Netz-Infrastruktur hat nur dazu geführt, dass sich die Angreifer mit den großen Tier-1 Carriern angelegt haben. Diese bilden das Rückgrat des Internets: was auf dieser Ebene gefiltert wird, kommt nicht mehr weit. Man könnte das auch so formulieren: Das Immunsystem des Internets wurde aktiv und hat den Angriff abgewehrt.
- Neben dem technischen Angriff gibt es immer auch den Kampf um die öffentliche Meinung und die Sympathien der breiten Bevölkerung. Die Aktion ließ sich anfangs noch als Kampf gegen Zensur verkaufen, aber mit den ersten Meldungen über Probleme für unbeteiligte Dritte wurde das immer schwerer haltbar.
- Je länger der Angriff dauert, umso mehr wird auch die Rückverfolgung klarer und eindeutiger. Damit riskiert die Koalition der Angreifer, dass deren Ressourcen (Netze, Server, Botnetze) bekannt werden und neutralisiert werden können.
  So etwa wurde der Organisation des Sprechers der Angreifer (Cyberbunker/CB3ROB) zeitweise ihre Netzanbindung abgedreht.
- Es ist klar, dass im Zuge der Angriffe Gesetze gebrochen wurden. Die internationale Gemeinschaft der Polizeibehörden wurde aktiv. Das mag dann für einige der Angreifer zu riskant geworden sein.

[13] http://cluepon.net/ras/gizmodo

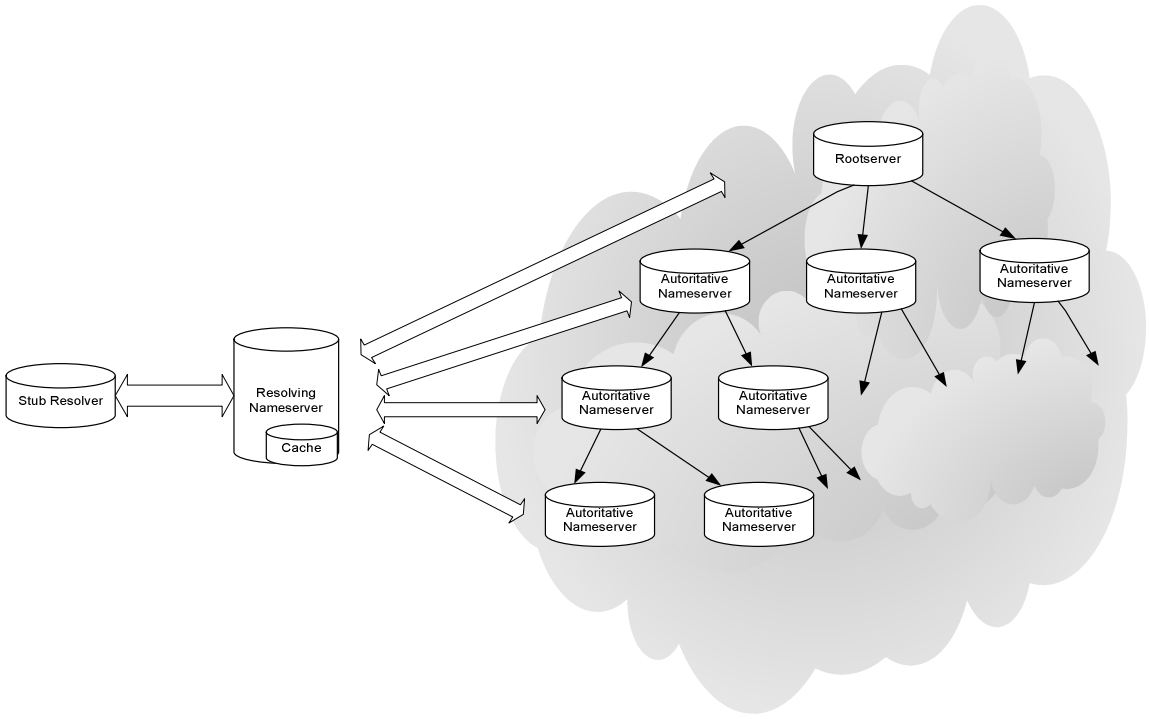
Angriffsmethode

Wie immer bei solchen Angriffen wurde ein Mix an verschiedenen Strategien und Methoden benutzt. Der Hauptanteil war in diesem Fall ein Amplification-Attack über offene, rekursive Nameserver. Dieser nutzt schlecht konfigurierte Geräte Dritter aus, um die Identität des Angreifers zu verstecken und die eigenen Angriffs-Kapazitäten zu verstärken.

Rekursive Nameserver

Das Domain Name System (DNS) ist die global verteilte Datenbank, die eine Umsetzung von Domainnamen („orf.at“, „www.ris.bka.gv.at“, „mail.example.com“, …) auf Routingparameter (IP-Adressen, Mailservernamen, Portnummern, …) erlaubt. Bei der Namensauflösung mittels DNS sind drei Komponenten im Spiel:

- Autoritative Nameserver: Diese Server sind für einen Teil des globalen Namensraumes zuständig und antworten auf Anfragen zu Hostnamen aus ihrem Verantwortungsbereich. Zu dieser Gruppe gehören die „Root-Nameserver“, die die Wurzel des DNS betreuen, die Nameserver der Top-Level-Domains (etwa „.at“ oder „.com“) und die Nameserver, die für die Domains einzelner Firmen verantwortlich sind.
- Stub Resolver: Das ist das Stück Software in jedem PC, Server, Smartphone, Tablett, Webcam, … , das Fragen an das DNS stellt: Dieser „Stub Resolver“ kann aber die Delegationsketten über die „autoritativen Nameserver“ nicht selber nachverfolgen, daher betreiben Firmen und ISPs immer auch:
- Rekursive (oder Resolving) Nameserver: Das sind Nameserver, die Anfragen der Stub Resolver entgegennehmen, die relevanten autoritativen Nameserver befragen, Antworten zwischenspeichern (deswegen auch „Caching Nameserver“ genannt) und dann die finale Antwort an die Stub Resolver zurücksenden.



DNS Amplification Attacks

Anfragen im DNS sind meist kleine Datenpakete in der Größe von 40 Bytes. Die Größe der Antworten kann stark variieren, in manchen Fällen können sie 3000 Bytes oder mehr erreichen. Das Protokoll mit dem diese Fragen meist gestellt werden, benutzt UDP (User Datagram Protocol) als Transportprotokoll, kann daher die Identität des Absenders nicht verifizieren.

Da die rekursiven Nameserver eine Dienstleistung für die Stub Resolver erbringen, werden normalerweise diverse technische Maßnahmen gesetzt, damit nur Fragen von berechtigten Stubs beantwortet werden. Die Erfahrung der letzten Wochen hat bewiesen, dass es global im Internet mehrere Millionen[14] rekursive Nameserver gibt, die eine solche Einschränkung nicht implementiert haben, und daher jedem Fragesteller eine Antwort zukommen lassen.

Dies haben sich die Angreifer zunutze gemacht. Ein solcher DNS Amplification / Reflection Attack funktioniert folgendermaßen:

1. Der Angreifer schickt eine (kleine) DNS-Anfrage an einen offenen rekursiven Nameserver. Dabei ist die Source-IP-Adresse nicht auf die des Angreifers gesetzt, sondern es ist die Adresse des Opfers eingetragen.

   Die Frage wird vom Angreifer so gewählt, dass die Antwort möglichst groß ausfällt.

2. Der rekursive Nameserver sucht sich die Antwort zusammen (wenn er sie nicht bereits im Cache hat), und schickt sie zurück. Wegen der gefälschten Source-IP-Adresse geht die Antwort nicht an den Angreifer, sondern an das Opfer.

3. Das Opfer sieht einen Schwall von großen DNS-Antworten, die potentiell seine Internetanbindung überlasteten. Dabei gilt:
   a. Die Absender-IP-Adressen, die das Opfer sieht, sind die der rekursiven Nameserver, nicht die des Angreifers.
   b. Dieses „über die Bande spielen“ des Angriffs verstärkt die Schlagkraft um einen Faktor bis zu 100.
   c. Es können tausende verschiedene rekursive Nameserver im Spiel sein. Das erschwert das Ausfiltern des Angriffs beim Opfer und verteilt die Last bei den rekursiven Namenserver soweit, dass sie nicht unbedingt negativ auffallen muss.

Weitere Informationen zu diesen Angriffen finden sich in RFC 5358[15] oder bei Team Cymru[16], die dazu auch ein Erklärungsvideo online gestellt haben. Auch von PCH gibt es ein Video dazu auf Youtube[17].

Diese Angriffsmethode ist bei weitem **nicht neu**, sondern ist schon lange bekannt und sie wird auch schon seit Jahren regelmäßig im Internet beobachtet.

[14] http://openresolverproject.org/
[15] https://www.ietf.org/rfc/rfc5358.txt
[16] https://www.team-cymru.org/Services/Resolvers/
[17] https://www.youtube.com/watch?v=Vlhu8_Aa7J8

Auswirkungen auf Österreich

Das BGP Hijacking dürfte sich nicht bis nach Österreich weitergesprochen haben: Als Route zu einer einzelnen IP-Adresse („/32“) wird diese an vielen Stellen ausgefiltert.

CloudFlare betreibt keinen Standort in Österreich, daher war der österreichische Teil des Internets auch nicht Ziel des Angriffs. Auch am Wiener Internet Exchange Point (VIX) wurden keinerlei auffällige Verkehrsmuster registriert.

Hingegen waren durchaus Rekursive Nameserver in Österreich an der Verstärkung / Reflexion der Angriffe beteiligt.

Das österreichische nationale Computer Emergency Response Team (CERT.at) ist in einige der globalen Kooperationsmechanismen eingebunden, über welche die Reaktion auf die Angriffe koordiniert wurden (Mailinglisten, Instant Messaging Systeme, Telefonkonferenzen).

Mit der Bereinigung aller falsch konfigurierten Nameserver wird das CERT – gemeinsam mit den ISPs – noch länger zu tun haben. Das wird eine Aufgabe für die nächsten Jahre werden.

Lektionen aus dem Angriff

Auch wenn Österreich bei diesem Vorfall nur peripher involviert war, so sind doch die Lehren daraus auch für uns wichtig. Keiner weiß, ob uns nicht der nächste Angriff deutlich stärker betrifft. Wir müssen daher in Vorbereitung auf das nächste Mal **jetzt** mit der Bereinigung der erkannten Problemfelder anfangen.

Technische Maßnahmen

Der Angriff nutzte einige technische Probleme aus, die man beheben sollte:

Absicherung der Routing-Protokolle

Um ein BGP-Hijacking zu unterbinden ist eine sorgfältige Konfiguration (und vor allen laufende Pflege) von Filterlisten in den Routern nötig. Vertrauen in die Peering-Partner an den Exchange Points und die eigenen Kunden ist zu wenig: es muss ja nicht immer böswilliges Fehlverhalten der anderen sein, gegen das man sein eigenes Netz schützen sollte, sondern auch gegen unabsichtliche Fehlkonfigurationen.

Eine kryptografische Absicherung der Routingprotokolle ist in Entwicklung[18]. Bis diese aber auch in der Praxis einsatzbereit ist, sollten alle ISPs sich die Richtlinien[19,20] zur Filterkonfiguration zu Herzen nehmen.

Control Plane Protection

In vielen Netzen konzentrierte man sich auf die Absicherung der Applikationen. Etwa ein Load-Balancer vor dem Webserver oder ein Anycasting [21] der Nameserver. Als in diesem Fall der Angriff dort nichts mehr erreichen konnte, schwenkten die Angreifer auf die darunterliegende Netzwerk-Infrastruktur um. Dort wird die „forwarding plane“ von der „control plane“ unterschieden: einmal

[18] https://www.ripe.net/lir-services/resource-management/certification/bgp-origin-validation
[19] https://tools.ietf.org/html/draft-ietf-opsec-bgp-security
[20] http://moo.cmcl.cs.cmu.edu/~dwendlan/routing/
[21] http://www.ipcom.at/dns/rcodezero_anycast/

geht es um die Pakete, die vom Router empfangen und weitergeleitet werden, während Pakete, die an den Router selber adressiert sind die „control plane“ betreffen. Im Normalfall gibt es nur ganz wenige, klar umrissene und abgegrenzte Fälle, in denen ein Router selber ansprechbar sein muss. Dies sollte auch dringend durch technische Maßnahmen eingeschränkt werden.

Es existieren genug Leitfäden, wie eine sichere Konfiguration eines IP-Netzwerkes auszusehen hat, damit dieses im Falle eines Angriffs robust reagiert. Siehe dazu etwa die Beispielskonfigurationen von Team Cymru[22], diverse Vorträge[23] aus NANOG – Konferenzen oder auch ein Dokument von Arbor Networks[24].

Falls ein kompetentes Operating des eigenen Netzes nicht machbar ist, sollte auf qualifizierte Dienstleister zurückgegriffen werden, wobei klar vertraglich definiert sein muss, wer für die Sicherheitsaspekte (Konfiguration, Operation, Vorfallsbewältigung) zuständig ist.

Im Falle der IXPs ergeben sich daraus mehrere Lektionen, die primär die Adressierbarkeit des IXP-Netzes betreffen. Ein Diskussionsprozess im Rahmen der Europäischen Vereinigung der IXP[25] wurde bereits angestoßen.

Network Hygiene

Um Wiederholungen des DNS Reflection / Amplification Angriffes zu unterbinden, sollte man folgende drei Bereiche adressieren:

1. Das Fälschen von Source-IP Adressen sollte auf Seite der ISPs unterbunden sein. Das ist nichts neues, das wird schon im Dokument „Best Current Practices (BCP) 38“[26] aus dem Jahre 2000 als wichtig genannt. Es wird wirklich Zeit, dass dies flächendeckend implementiert und auch überprüft wird.

2. Rekursive Nameserver sollten nicht offen für die Welt sein, siehe dazu RFC5358[27]. Auch das ist schon länger bekannt, und muss nur endlich überall umgesetzt werden.

   Wie man die offenen rekursiven Nameserver in seinem eigenen Netz findet, beschreibt das US-CERT in TA13-088A[28], ein CERT.at Mitarbeiter hat dazu auch ein Tool veröffentlicht[29].

   Meist handelt es sich dabei um CPEs[30] (consumer premises equipment; z.B. WLAN Router/Modems), deren Software nur selten aktualisiert wird.

3. Auch autoritative Nameserver können für Amplification Attacks benutzt werden; das wird auch bereits im Internet beobachtet. Deren Missbrauch zu verhindern ist nicht ganz so

[22] https://www.team-cymru.org/ReadingRoom/Templates/
[23] http://www.nanog.org/meetings/nanog54/abstracts.php?pt=MTg4NCZuYW5vZzU0&nm=nanog54
[24] https://www.box.com/s/osk4po8ietn1zrjjmn8b
[25] https://www.euro-ix.net/
[26] https://tools.ietf.org/html/bcp38
[27] https://www.ietf.org/rfc/rfc5358.txt
[28] https://www.us-cert.gov/ncas/alerts/TA13-088A
[29] https://github.com/aaronkaplan/open-recursor-check
[30] https://www.nytimes.com/2013/03/30/technology/devices-like-cable-boxes-figured-in-internet-attack.html?_r=2&pagewanted=all&

einfach wie bei den Rekursiven, es gibt dazu aber schon sehr effektive technische Maßnahmen, etwa Response Rate Limiting[31].

Rückverfolgung von gefälschten Paketen

Um bei solch einem Angriff den eigentlichen Auslöser zu finden, müssen die IP-Pakete mit den gefälschten Absenderadressen rückverfolgt werden können. Das ist technisch durchaus machbar, bedarf aber einiger Vorarbeiten. Dazu gehört primär ein gutes Netzwerkmanagement, das nicht nur auf die Auslastung des Netzes fokussiert ist, sondern auch eine Analyse der Verkehrsströme erlaubt. Das muss nicht unbedingt teuer sein, es existieren auch Open Source Lösungen wie etwa „nfdump/nfsen“[32], die für mittelgroße Netze (netflow-fähige Router vorausgesetzt) ausreichend sind.

Das Rückverfolgen von gefälschten Paketströmen über IXPs hinweg ist technisch deutlich schwieriger, sollte aber auch angegangen werden.

Neben dem technischen Werkzeug ist auch entsprechend geschultes und geübtes Personal nötig.

Organisatorische Maßnahmen

Hier sind vor allem zwei Aspekte wichtig:

- Zusammenarbeit zwischen den ISPs und der Internet Security Community. Mit dem Austrian Trust Circle, dem Programm von CERT.at zur Einbindung der strategischen Infrastruktur wurde hier schon ein erster, wichtiger Schritt gesetzt. Die ISPs mögen im Markt als Konkurrenten auftreten, wenn es aber um die Stabilität des Internets geht, muss auf technischer Ebene kooperiert werden.

  Die Zusammenarbeit mit CERT.at hilft hier, die Brücke zwischen der lokalen Internet-Gemeinde und der globalen IT/Internet-Security Community zu schlagen.

- Die oben genannten technischen Maßnahmen sind nicht gratis: das alles umzusetzen, laufend zu warten, und **regelmäßig zu überprüfen** benötigt nicht unerhebliche Ressourcen. Es braucht daher Verständnis, Unterstützung und auch ein Einfordern dieser Maßnahmen von Seiten des Managements.

[31] http://www.redbarn.org/dns/ratelimits
[32] http://sourceforge.net/projects/nfsen/

Allgemeine Fragen

Dieser eskalierende Streit zwischen zwei Fraktionen im Netz wirft aber neben den technischen Fragen zur Unterbindung und Abwehr solcher Angriffe auch einige Fragen auf, die den Streit selber thematisieren und wie die Gesellschaft darauf reagieren sollte.

Diese Fragen sollen nur als Denkanstoß dienen, und werden daher hier nicht beantwortet.

- Was ist bei der Strafverfolgung im Internet falsch gelaufen, dass strafbares Verhalten (Spamming, Betrieb von Cybercrime-Infrastruktur, …) an vorderster Front von Spamhaus & co bekämpft wird, und nicht von den legitimierten, staatlichen Autoritäten? Dass sich Mailserverbetreiber auf die Blocklisten von Spamhaus als Schutz von der Spamlawine stützen müssen?
- Ist es legitim, dass Spamhaus in seinen Listen nicht nur die Spammer selber listet, sondern auch Organisationen, die eine Geschäftsbeziehung zu diesen nicht sofort abbrechen können oder wollen? Wie verträgt sich das mit dem Grundrecht auf Internetzugang, und dem Quasi-Kontrahierungszwang mancher Basisinfrastrukturanbieter?
- Hat Stophaus recht, wenn sie behaupten, dass Spamhaus zu viel Macht hat? Dass Spamhaus eine Art Zensurbehörde geworden ist, die über Erpressung der ISPs ihren Willen durchsetzen kann?
- Was ist der datenschutzrechtliche Aspekt solcher Listen? Besteht hier Regulierungsbedarf analog zu den Kreditschutzverbänden?
- Ist bei der Abwehr des Angriffes auch auf die Strafverfolgungsaspekte eingegangen worden? Oder haben die Netzbetreiber das Problem als ein primär technisches eingestuft, das auch rein technisch zu lösen war? Wurde zeitnah Anzeige erstattet? Hat die Einschaltung der Polizeikräfte bei der Ausforschung der Urheber des Angriffs geholfen?
- Hat man sich zu sehr auf die reaktive Abwehr konzentriert und zu wenig auf die Rückverfolgung?
- Wie sollte man reagieren, wenn sich herausstellt, dass die Angreifer in Ländern agieren, mit denen es keine vernünftige Zusammenarbeit in Bezug auf Cybercrime gibt?
- Wie sind die offenen rekursiven Nameserver rechtlich zu betrachten? Welche Haftungen können sich aus dieser unbewussten Mithilfe an einer Straftat ergeben?
- Wie ist der technische Stand der österreichischen ISPs? Haben alle (oder wenigstens die großen) die notwendigen technischen und organisatorischen Absicherungen umgesetzt?
- Bedarf es weiterer Maßnahmen, damit ein etwaiger ähnlicher Vorfall – mit Fokus auf Österreich – kooperativ zwischen allen ISPs gelöst werden könnte? Wie kann man die internationalen Backbonebetreiber (für die Österreich ein fast irrelevanter Mark ist) auch zur Mitarbeit verpflichten?