CLOUDMARK®

Intelligent Network Security

Security Threat Report

2015 Q1

Table of Contents

Acquinity Interactive: The Rise and Fall of a Spam Empire

Documents revealed by several lawsuits involving Acquinity Interactive and its predecessor, ModernAd Media, give an unusually detailed view into the finances of a spammer. At its peak, Acquinity generated approximately $147 million in revenue per year,[1] an income of $17 million,[2] and claimed to employ six hundred people.[3] The president of Acquinity, Garry Jonas, had a flamboyant lifestyle. He owned a $2,300,000 waterfront condo in Boca Raton, Florida[4] and went into partnership as a boxing promoter with former heavyweight champion Mike Tyson.[5] However, Acquinity, Jonas, and three of Acquinity's four largest customers all fell afoul of the law for various illegal or deceptive business practices.[6]

This operation was not a single corporation, but a complex web of related corporations and individuals working in concert on various legal and illegal Internet marketing schemes. In fact, there was not even a single entity called Acquinity, but two: Acquinity Interactive, LLC, a Florida limited liability company and 7657030 Canada, Inc., a Canadian corporation that was also doing business as Acquinity Interactive in the lawsuit that brought down this operation, the FTC grouped these two corporations, along with Garry Jonas, the President of Acquinity Interactive, LLC, and three other individuals (Scott Modist, Joshua Greenberg, and Gregory Van Horn) collectively as the Acquinity Defendants.[7] Modist and Greenberg were later dropped from the case.[8]

7657030 Canada was registered in September of 2010, with Garry Jonas listed as the sole director.[9] However, the story goes back further than that. Jonas, Van Horn and Modist were previously executives of ModernAd Media, LLC,[10] a Florida Corporation registered in May, 2008.[11] Jonas was the CEO, and Warren Rustin, an old high school friend of his, was President.[12] It did not take long for ModernAd Media to get into trouble with the law. In May of 2010 they were fined $2.9 million

[1] Acquinity Interactive, LLC income tax return for 2011, court document from Pulsepoint, Inc. v. 7657030 Canada, Inc. et al https://drive.google.com/file/d/0Bx9WQt2m2YU-QzdEU1VTTFhKYkk/view?usp=sharing
[2] Ibid.
[3] "Acquinity, which is based in Florida, employs about 600 people at its Deerfield Beach facility, said A.J. Rosenfield, the company's vice president of human resources in Arizona." http://archive.azcentral.com/community/gilbert/articles/2011/10/17/20111017gilbert-new-call-center.html
[4] Federal Trade Commission vs. Acquinity Interactive et al. Stipulated Final Order https://www.ftc.gov/system/files/documents/cases/141022revenuedeforder.pdf [PDF]. Zillow.com listing.
[5] http://en.wikipedia.org/wiki/Iron_Mike_Productions
[6] Full details below.
[7] Federal Trade Commission vs. Acquinity Interactive et al. Amended Complaint https://www.ftc.gov/system/files/documents/cases/140707revenuepathcmpt.pdf [PDF]
[8] Federal Trade Commission vs. Acquinity Interactive et al. Order Granting Motion for Voluntary Dismissal https://www.ftc.gov/system/files/documents/cases/141022revenuedismissalorder-greenberg.pdf [PDF]
[9] Corporations Canada https://www.ic.gc.ca/app/scr/cc/CorporationsCanada/fdrlCrpDtls.html?corpId=7657030
[10] Adams vs ModernAd Media et al. First Amended Complaint. https://ecf.cod.uscourts.gov/doc1/03913956680 [registration required]
[11] http://www.bizapedia.com/fl/MODERNAD-MEDIA-LLC.html
[12] Adams vs ModernAd Media et al. First Amended Complaint. https://ecf.cod.uscourts.gov/doc1/03913956680 [registration required]

by the Florida Attorney General bring charges for violations of the CAN-SPAM law.[13] As part of the settlement, ModernAd Media signed an Assurance of Voluntary Compliance (AVC) regulating its future business practices.[14] It's clear from the AVC that the attorney general's office wished to prevent ModernAd Media from offering 'free' goods that in fact came with a lot of strings attached.

The AVC was only binding for ModernAd Media and not the individuals involved. Perhaps this is the reason that in December 2010 Rustin announced that he had:

> *...recently sold certain assets of ModernAd Media to a group of ModernAd executives that includes our former CEO Gary Jonas, Greg Van Horn and Josh Greenberg. They have formed an Internet marketing company named Acquinity Interactive...*[15]

In fact, it appears as if all the assets were transferred to Acquinity, including approximately $10 million in accounts receivable, and customers accounting for approximately $120 million in annual revenue,[16] which one disgruntled creditor described as the "fire sale price" of $2,682,783.00.[17] Acquinity took over ModernAd Media's operations on January 1st, 2011, operating out of the same address at 2200 SW 10th Street, Deerfield Beach, Florida.[18]

One of the assets transferred from MobileAd Media to Acquinity appears to have been their list of consumer email addresses. Both companies practiced "co-registration", which is a process of collecting an email address purportedly for one purpose while incidentally signing that email address up for additional marketing messages.[19] Acquinity claimed to have a list of 80,000,000 email addresses with 150,000 new registrations per day and offered to rent their list for unlimited use to other email marketers.[20] Acquinity's aggressive registration and email marketing policies meant

[13] http://emailexpert.org/modernad-media-fined-2-9-million-for-can-spam-violations/
[14] 'The AVC requires that ModernAd Media not: (1) use words that reasonably lead a person to believe that he or she may receive something of value for free without "clearly and conspicuously disclosing the material terms, conditions and obligations" of each offer; nor (2) use words such as "Test and Keep" or "Try and Keep" in emails that suggest something of value will be given in exchange for testing or trying that item without clearly and conspicuously warning the consumer of the existence of additional obligations in both the subject line and the body of the emails. ModernAd Media also agreed: (1) to disclose clearly and conspicuously any and all material information that would help consumers make informed decisions before purchasing merchandise or participating in trial offers; (2) to place a link to the terms and conditions of the advertised offer on every webpage; (3) to place a link labeled "Get Status" that allows consumers to access current information about the consumer's account specifically related to the offer; (4) to cease using prechecked boxes for acceptance of terms and conditions; (5) not to require consumers to qualify for a creditbased sponsor's offer, such as a credit card, in order to receive the gift; and (6) to clearly state the minimum amount of time a consumer must be subscribed in order to receive the gift for subscription-based offers. In addition, ModernAd Media must disclose its corporate name and contact information on all webpages, even if the page is operated by a third party contractor. The AVC also contains record keeping provisions that will help the Florida Attorney General's Office monitor the company for compliance with the terms of the agreement.' http://www.troutmansanders.com/files/FileControl/fdac7efc-3ebf-4ca5-bb03-65426dd0d1da/7483b893-e478-44a4-8fed-f49aa917d8cf/Presentation/File/summer2010consumer.pdf [PDF]
[15] Adams vs ModernAd Media et al. First Amended Complaint. https://ecf.cod.uscourts.gov/doc1/03913956680 [registration required]
[16] Ibid.
[17] Pulsepoint, Inc. v. 7657030 Canada, Inc. et al. Complaint.
[18] Ibid.
[19] Ibid.
[20] http://www.kinnamon.com/documents/KinnamonAcquinityListRental.pdf [PDF]

that spam filters stopped many of their emails.[21] By using a variety of techniques for avoiding filters, they were able to get enough emails delivered to make some income from legitimate advertising affiliate programs. However, some of their largest clients were less legitimate.

A court case brought by a creditor of ModernAd media resulted in disclosure of Acquinity's earnings by customer and year for a three-year period.[22] Here are Acquinity's top four sources of income.

Client	2011	2012	2013 Jan-Nov	TOTAL
Frontline Direct	$14,226,851	$12,693,673	$7,034,438	$33,954,961
One Technologies, L.P.	$8,397,392	$8,110,505	$4,809,919	$21,317,816
Polling Associates	$14,118,885	$5,634,021	$621,462	$20,374,368
Zbiddy/Ecom Interactive	$8,088,923	$11,076,409	$389,133	$19,554,464

Frontline Direct is a legitimate affiliate marketing program.

According to an FTC press release from November 2014, One Technologies, L.P. operated:

> *...an online scheme that allegedly lured consumers with "free" access to their credit scores and then billed them a recurring fee of $29.95 per month for a credit monitoring program they never ordered.*[23]

One Technologies generated $21 million in revenue for Acquinity over three years.

Polling Associates is a corporation with a mailing address in the tiny Caribbean country Saint Kitts and Nevis.[24] Along with its operators, Burton Katz and Jonathan Smyth, it was included in the FTC's Amended Complaint against Acquinity.[25] According to the FTC, they worked with Acquinity to trick mobile phone users into signing up for services that resulted in unauthorized charges on their phone bill,[26] a process known as phone "cramming". There is evidence to suggest that Garry Jonas may have been behind this scheme. According to testimony on phone cramming delivered to the Senate Committee on Commerce, Science and Transportation in 2011:

> *MORE [International] explained that Gary [sic] Jonas and Jeff McKay, the owners of ModernAd Media and The Payment People, respectively, "directed the formation" of the third-party vendors and "identified individuals to serve as presidents."*[27] *Like third-party vendors related to daData and MySnS, these third-party vendors were also one common enterprise... Committee staff has found ample evidence suggesting that the third-party vendors related to daData, MySnS, and MORE International were nothing more than*

[21] Cloudmark Global Threat Network.
[22] Court document from Pulsepoint, Inc. v. 7657030 Canada, Inc. et al https://drive.google.com/file/d/0Bx9WQt2m2YU-M1o2T3ZtT0Zvdjg/view?usp=sharing
[23] https://www.ftc.gov/news-events/press-releases/2014/11/ftc-illinois-ohio-stop-scheme-offered-free-credit-scores-then
[24] Court document from Pulsepoint, Inc. v. 7657030 Canada, Inc. et al https://drive.google.com/file/d/0Bx9WQt2m2YU-M1o2T3ZtT0Zvdjg/view?usp=sharing
[25] Federal Trade Commission vs. Acquinity Interactive et al. Amended Complaint https://www.ftc.gov/system/files/documents/cases/140707revenuepathcmpt.pdf [PDF]
[26] Ibid.
[27] Footnote in original Senate document: Letter from Linda Goldstein, counsel to MORE International, to Erik Jones, counsel to the Senate Commerce Committee (Mar. 24, 2011)

> *"front companies" for larger "hub companies." Committee staff found third-party vendors operating out of mailboxes in UPS Stores, Post Office boxes, fake offices, and residences, with "presidents" that knew nothing about the companies they were supposedly leading.*[28]

Polling Associates generated $20 million in revenue for Acquinity over three years. In addition, a company called W Media generated $7 million in revenue for Acquinity in two years with no apparent assets other than a PO Box in New Jersey,[29] so this may have been another front company.

Ecom Interactive owned Zbiddy.com,[30] a "penny auction" site. Penny auctions claim to auction goods at far less than retail prices. However, the bidders pay a fee for each unsuccessful bid, netting the seller a large profit.[31] The Better Business Bureau called penny auctions one of the top ten scams of 2011.[32] Users of Zbiddy also complained of overbilling and poor quality goods.[33] The BBB gives Zbiddy an F rating, citing 618 complaints filed and the fact that "Business has failed to resolve underlying cause(s) of a pattern of complaints."[34] It appears that Acquinity owned a significant interest in Ecom Interactive/Zbiddy. Coincidentally, Zibddy operated out of the same address in Deerfield, Florida[35] as Acquinity and ModernAd Media, and is listed as a "Non-includable US Entity" on Acquinity's 2011 tax return.[36] A blog comment from someone claiming to be a former employee confirms that Garry Jonas was one of the principal operators of Zbiddy.com.[37] In January 2013, following an investigation by the Florida Attorney General's Office, Ecom Interactive signed an Assurance of Voluntary Compliance prohibiting overbilling, shill bidding and other bad practices.[38] Zbiddy generated $19.6 million in revenue for Acquinity over three years.

In the end, it was the same scam that ModernAd Media operated that brought Acquinity down — offering "free" gift cards and consumer goods that never actually turned up. In July 2013 the FTC

---

[28] UNAUTHORIZED CHARGES ON TELEPHONE BILLS: WHY CRAMMERS WIN AND CONSUMERS LOSE. HEARING before the COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION. UNITED STATES SENATE, ONE HUNDRED TWELFTH CONGRESS, FIRST SESSION, JULY 13, 2011. http://www.gpo.gov/fdsys/pkg/CHRG-112shrg71640/html/CHRG-112shrg71640.htm

[29] Court document from Pulsepoint, Inc. v. 7657030 Canada, Inc. https://drive.google.com/file/d/0Bx9WQt2m2YU-M1o2T3ZtT0Zvdjg/view?usp=sharing

[30] http://www.myfloridalegal.com/EC_Edoc.nsf/Enforcement/5A8F471BE13FD1D185257B1000651A65

[31] http://blog.cloudmark.com/2012/02/06/valentines-day-penny-auctions-and-the-prisoners-dilemma/

[32] http://www.bbb.org/blog/top-scams-of-2011.html

[33] http://www.complaintslist.com/websites/auction/zbiddy/, http://www.ripoffreport.com/r/ZBiddy/Deerfield-Beach-Florida-33442/ZBiddy-Deceptively-and-Fraudulent-took-funds-from-credit-card-Deerfield-Beach-Florida-1095106

[34] http://www.bbb.org/delaware/business-reviews/penny-auctions/zbiddy-com-online-auction-in-deerfield-bch-fl-32003738/

[35] http://www.ripoffreport.com/r/ZBiddy/Deerfield-Beach-Florida-33442/ZBiddy-Deceptively-and-Fraudulent-took-funds-from-credit-card-Deerfield-Beach-Florida-1095106

[36] Acquinity Interactive, LLC income tax return for 2011, court document from Pulsepoint, Inc. v. 7657030 Canada, Inc. et al. https://drive.google.com/file/d/0Bx9WQt2m2YU-QzdEU1VTTFhKYkk/view?usp=sharing

[37] "But the real operators behind zBiddy are right in the state of Florida. One is Garry Jonas the CEO of Acquinity Interactive in Deerfield Beach. Jonas is currently being sued by the FTC. They are trying to close him down for spamming phone numbers for zBiddy and free Walmart and Best Buy gift cards. Acquinity does the SMS spamming and runs all the traffic to generate the leads to the zBiddy site." https://logicalabstracts.wordpress.com/2012/11/30/penny-auctions-are-gambling/

[38] http://www.myfloridalegal.com/EC_Edoc.nsf/0/5A8F471BE13FD1D185257B1000651A65/$file/zBiddy+com_Ecom+Interactive+AVC.pdf [PDF]

filed suit against Acquinity and others for sending spam SMS messages.[39] According to the FTC's press release:

> *Consumers who clicked on the links in the messages found themselves caught in a confusing and elaborate process that required them to provide sensitive personal information, apply for credit or pay to subscribe to services to get the supposedly "free" cards. In addition, consumers' phone numbers were signed up to receive unwanted automated telemarketing calls, also known as robocalls.*[40]

According to a former Acquinity employee posting on Glassdoor.com:

> *The calls themselves were pitiful because we're taking inbound calls for people claiming a gift basket when all they're doing is eventually getting looped into buying something. We had to "review" a supposed online survey they took which asked way too much psychographic information bordering on intrusive. The key question that made the difference was asking if the caller had a credit card, bank debit card, both or neither. If they had both and not a prepaid card, you're forced to pitch a 14 day trial for $3.95 and get the credit card info on the spot while fighting objections.*[41]

The FTC's initial complaint requested a temporary injunction freezing the assets Acquinity and the other defendants, and appointing a receiver in order to "...avert the likelihood of consumer injury during the pendency of this action."[42] This appears to have effectively put Acquinity out of business. Moreover, their earnings for 2013 were less that half those of 2012.[43] The case settled in October 2014, upon which the Acquinity defendants were required to pay a $7.8 million fine, refrain from spamming and cease other illegitimate marketing practices. Further, they were required to make regular reports to the FTC on all their business activities. To ensure payment of the fine, the FTC placed a lien on Jonas's condo and obtained rights to assets owned by Kare Pharmacy, another business associated with Acquinity.[44]

Jonas's star continues to fall since the settlement. In December 2014, it was announced that the boxing promotion company that he founded with Mike Tyson was breaking up.[45] Perhaps his brand is so tarnished that even Mike Tyson does not want to do business with him.

[39] https://www.ftc.gov/news-events/press-releases/2013/07/ftc-acts-against-spam-text-robocalling-operations
[40] Ibid.
[41] http://www.glassdoor.com/Reviews/Acquinity-Interactive-Reviews-E439857.htm
[42] https://www.ftc.gov/sites/default/files/documents/cases/130729revenuepathcmpt.pdf
[43] Court document from Pulsepoint, Inc. v. 7657030 Canada, Inc. et al https://drive.google.com/file/d/0Bx9WQt2m2YU-M1o2T3ZtT0Zvdjg/view?usp=sharing
[44] https://www.ftc.gov/system/files/documents/cases/141022revenuedeforder.pdf
[45] http://espn.go.com/blog/dan-rafael/post/_/id/11377/tysons-promotional-company-on-the-rocks

Country Report: Canada

Canada's New Anti-Spam Law Causes Big Reduction in Email Activity

On July 1st of last year, a stringent anti-spam law, Canada's Anti-Spam Law (CASL), went into effect[46] We took a look to see what impact this had on Canadian email activity.[47] Our most significant findings were:

- 37% reduction in spam originating in Canada, the majority of that going to the United States
- 29% reduction in all email received by Canadians, spam and legitimate
- No significant change in the percentage of emails received by Canadians that were spam

Let's look at those results in detail.

Spam is an international phenomenon, but the US is both one of the biggest sources and the biggest targets for spammers. It's not a surprise, then, that 53% of spam that Canadians receive is from the US, and 78% of spam that is sent from Canada goes to the US. However, the amount of spam outbound from Canada went down noticeably when CASL was implemented.

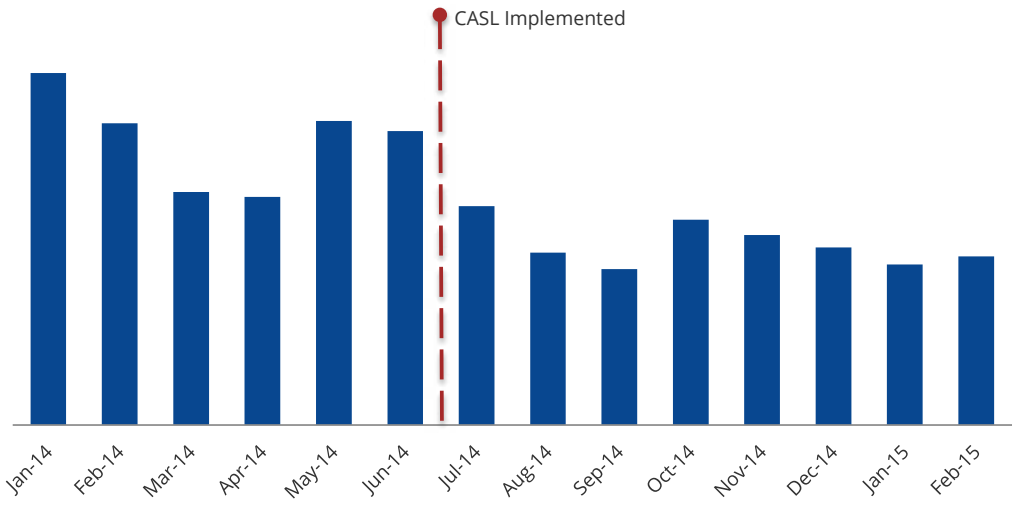

Fig. 1: *Spam Originating in Canada*

Though there is volatility from month to month, the total volume of spam originating in Canada every month since CASL was implemented had been lower than the lowest month before the law went into effect. The average monthly spam volume decreased by 37% and there was a dramatic drop in email received by Canadians following the implementation of CASL.

[46] http://blog.cloudmark.com/2014/07/10/canadian-anti-spam-law-casl-a-good-step-but-not-the-end-of-spam/

[47] Statistics are from spam detected by Cloudmark Authority. This filter usually runs after other spam filters based on IP address blocking etc., so total spam volumes may be higher. However, relative levels are a good measure of changes in activity. See http://blog.cloudmark.com/2013/07/09/lies-damn-lies-and-spam-statistics/

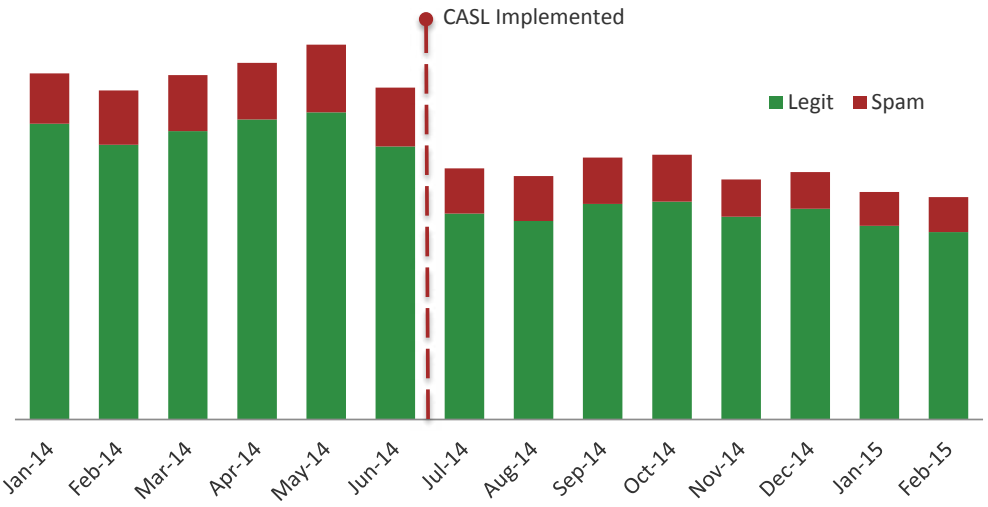

Fig. 2: *Email Received in Canada*

The monthly average volume for all email received by Cloudmark customers in Canada went down by 29% after CASL. This was split evenly between spam and legitimate email. The average percentage of email that was spam increased by an insignificant amount, from 16.5% to 16.6%.

Why did CASL have such an impact on legitimate email? Most likely because it enforces far more stringent requirements for obtaining consent for marketing emails. Practices for adding a consumer email address to a mailing list that would be acceptable under the US CAN-SPAM legislation do not satisfy the level of affirmative consent required by CASL. While CASL has been ineffective in preventing the professional spammers promoting bootleg pharmaceuticals, diet pills and adult services, it has stopped unscrupulous email marketers from growing their mailing lists by co-marketing or easy-to-miss opt out checkboxes.

CASL has even had an impact on some US spammers. We frequently see affiliate spam these days which contains the warning, “This message is not intended for Canadian citizens.”

Blocked IP Address by Country

Substantial Improvements in Panama and Romania, But a Disturbing Increase in Saudi Arabia

Generally the news is good this quarter. Worldwide we have seen widespread action to clean up spam sending systems resulting in a 13% decrease in the number of IPv4 addresses blacklisted by Cloudmark. The US remains the country with the most blocked IP addresses, but in the past three months, it too has seen a reversal of the increasing trend that dominated the previous two years. Let's hope that is sustained.

Romania, for a long time a major source of spam, continues to show dramatic improvement. Between November 2012 and April 2014, Cloudmark was blocking between 20% and 25% of Romania's entire IP address space. This is now down to 6.2%. While this is still high, it does represent significant progress in the past year. Romania is now in fifth place in terms of the absolute number of IP addresses blocked, after the US, China, Germany, and Russia.

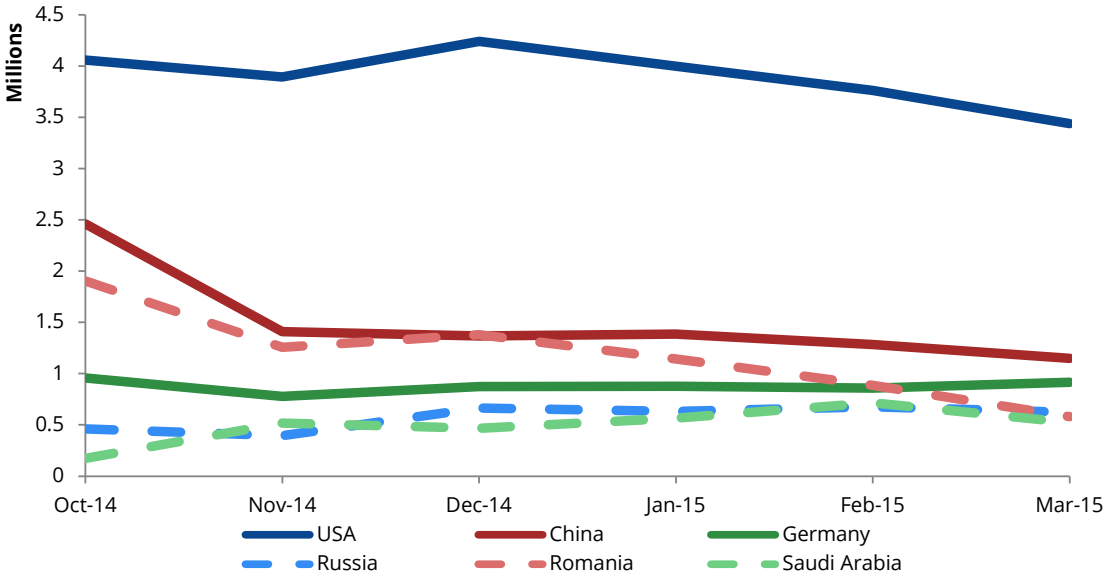

Fig. 3: *Blocked IP Address Count By Country*

Another dramatic improvement recently has been in Panama. Though Panama has a relatively low number of IP addresses in absolute terms, until January of this year Cloudmark was regularly blocking more than 10% of them, mostly due to the efforts of one hosting provider, Panamaserver.com. However, this year we have seen a large drop in the spam originating from this network, and when we do see attacks they are usually brief rather than running for days or weeks. As a result, we are currently blacklisting only 1.5% of Panama's IP addresses. This highlights the importance of

outbound spam filtering to preserve IP address reputation.

In terms of the percentage of IP addresses blocked, a relatively new arrival has taken the top spot.[48] Saudi Arabia now has 6.4% of their total address space blocked.

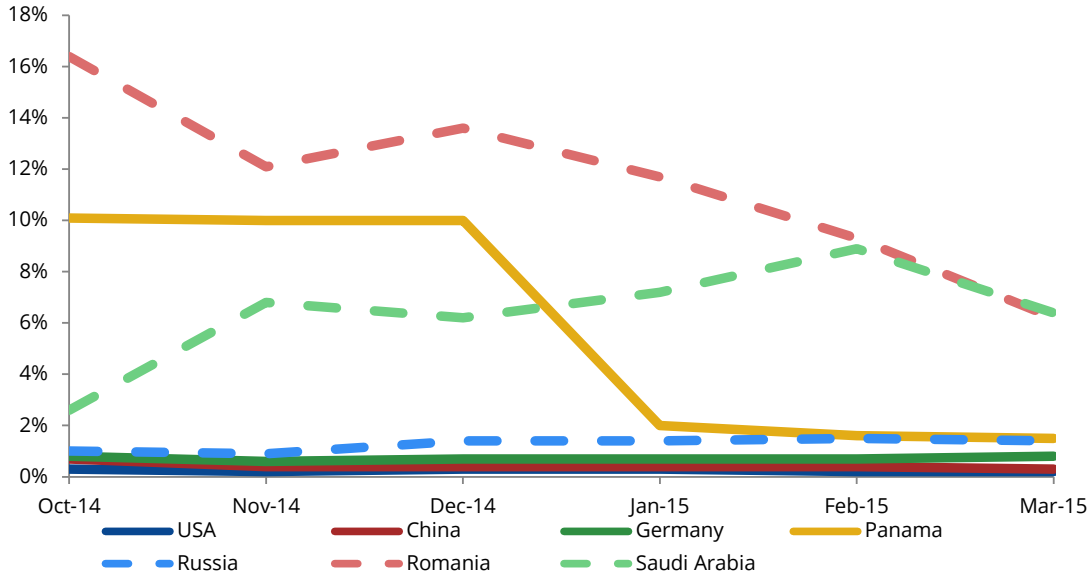

Fig. 4: *Percentage of IP Address Space Blocked by Cloudmark*

This is largely due to a single ISP, Saudinet, which is the largest in the region. It appears to be the result of widespread botnet infections and compromised accounts rather than the situation in Romania and Panama where resources were purchased by spammers. In Saudi Arabia, we saw a decline in the figures for March 2015, so hopefully Saudinet is getting a handle on their users' malware problem.

[48] Other countries with very small IP address spaces may have higher percentage of blocked IP addresses, but we do not report on these as they are not a significant source.

Ransomware: Getting Your Data Back

Every day, thousands of computers are infected with a particularly nefarious form of malware called "ransomware". This malware encrypts all the user's data and personal files, and will not decrypt them until the victim pays a ransom, usually in bitcoins. Hundreds of times a day, owners feel they have no alternative but to submit to this extortion.[49] Usually this is because it is critical data needed for work and the most recent backup may be out of date. Rather than lose days of work recreating the encrypted files, it is easier just to pay up. However, the victim may still lose days of work before the data is recovered because of the time required to obtain the bitcoins necessary to pay the ransom. In this article we look at the best way to obtain bitcoins in order to recover irreplaceable data as quickly as possible.

Paying ransom should be regarded as a last resort. It sends money directly to cyber criminals and thus encourages more criminal activity. It is far better to follow best practices to reduce the risk of infection, and allow easy recovery from backups in the event that you do get infected. However, not every consumer or enterprise follows best practices, and even law enforcement has fallen victim to ransomware. One local police department in Swansea, Massachusetts was forced to pay ransom when a computer containing police reports and booking photos was infected.[50]

There are several public exchanges that sell bitcoins, so it might seem that it would be easy to simply go to one and make a purchase on the Internet, as you would for any other goods or service. However, bitcoin transactions are irreversible and untraceable, so instant bitcoin purchases would provide an easy way for criminals to cash out stolen credit cards or bank account credentials. Further, the exchanges have responded to the threat of fraud by stringent identity checks, low purchase limits, and high transaction costs. The typical ransom is two bitcoins, so we set out to purchase two bitcoins as quickly as possible to ascertain the challenges a user may encounter. We were not particularly successful, but at the end of a week we had a clear idea of what we should have done.[51]

For same day purchases we found that Coin.Mx offered the best solution. This allows credit card purchases up to $500 after a validation process that, in addition to the usual identity checks, requires the purchaser to make a video showing their face, a government issued ID and both sides of the credit card used to make the purchase. Though it might be possible to cheat this process with a fake ID and stolen credit card, at least they would be able to share your picture with law enforcement if

[49] http://us.norton.com/ransomware/article
[50] http://www.heraldnews.com/x2132756948/Swansea-police-pay-750-ransom-after-computer-virus-strikes
[51] This article describes the use of bitcoin exchanges for low value purchases of bitcoins for immediate use. Cloudmark makes no warranty as to the security or reliability of the exchanges mentioned, or their suitability for this or other purposes. In the past, other bitcoin exchanges have experienced theft, fraud, and bankruptcy.

necessary. Initially the credit card company blocked the purchase transaction as suspicious and it took a phone call to get approval.

Coin.Mx offers a poor exchange rate and charges a hefty premium for credit card use. As a result, our $500 only purchased about 1.57 bitcoins, which was not enough to pay the ransom. The easiest way to deal with this is to ask a second person to sign up to Coin.Mx and pool resources to come up with the two bitcoins plus a little extra for the 0.001 bitcoin transaction fees that Coin.Mx charges. Alternatively, Coin.Mx will increase your purchase limits if you arrange a conference call with your bank.

If you have more time to spend, you may get better exchange rate from Coinbase.com. Once you have validated a bank account and credit card with them you can also make instant purchases, but this is limited to $100, which came to 0.37 bitcoins. (Adding that to the Coin.Mx instant purchase gave us a total of 1.94 bitcoins, frustratingly just short of the 2.00 bitcoin target.) You can however purchase bitcoins by bank transfer if you are prepared to wait several business days for the transaction to clear.

There are also websites that will broker instant purchases of bitcoins from people in your physical vicinity by arranging to meet in person and exchange bitcoins for cash. Even in a high tech region such as San Francisco we found that these meetings had a very high no-show rate. Further, we cannot recommend this approach unless you absolutely need to make your purchase without an audit trail.

Best Practices for Avoiding Ransomware:

- Keep your operating system, browser, anti-virus software, and applications up to date
- Don’t click on links or open attachments in unsolicited email
- Be on the lookout for phishing and spear phishing messages that appear to come from a trusted source
- Back up your data regularly
- If your data is mission critical, use an automated cloud-based system, so that your backups are always current and you can restore your computer to its status before any infection took place
- Test your restore process, to make sure that you really can recover your data in a reasonable time

Top Mobile Attack Types

Many countries continue to see SMS campaigns similar to those of 2014's latter months. However, gambling ads aimed at U.K. SMS inboxes have jumped by over 350% during the first quarter of 2015.

Churn and Burn Affiliate Casino Spam in the U.K.

Payday loan and accident compensation spam still remain the most popular forms of mobile messages reported by U.K. subscribers with 34 and 27 percent, respectively, of reports this quarter. The third highest form comes from mobile and online gambling sites and the affiliates advertising for them. This category has perennially been of low volume, accounting for only four percent of all reported U.K. mobile messages in 2014. These gambling site ads have risen from 5% in January to 21% in March.

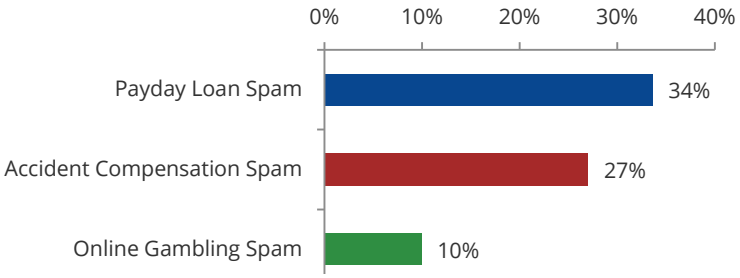

Fig. 5: *Top Forms of Unsolicited U.K. SMS, 15Q1*

Interestingly, it appears that this surge in March was due in large part to a single affiliate spammer (or small group coordinating the campaign.) Online gambling in the Great Britain is a very big and legitimate business. One such online gambling company is BGO Entertainment.

BGO has quite the marketing budget, bringing in the likes of movie star Verne Troyer and Twitter star Dan Bilzerian for their most recent $15 million series of video ads.[52] BGO also uses affiliates to drive traffic to their site. Through their BGO Buddies program, affiliates are guaranteed a portion of revenue generated from customers the affiliate refers to BGO's online casinos. Gambling affiliate programs are sophisticated and numerous enough that an entire ecosystem has developed around online casino affiliate programs. In October of last year, BGO partnered with affiliate marketing platform provider Income Access to provide BGO Buddy affiliates with easy-to-use geo, time-of-day, browser and other forms of highly targeted advertising.[53] However, BGO re-launched this program at the end of February following a move to Income Access's acquisition platform.

[52] http://www.vcpost.com/articles/31242/20141108/dan-bilzerian-verne-troyer-star-new-bgo-commercial-posts-more.htm
[53] http://www.igamingbusiness.com/news/bgo-entertainment-links-income-access

"We're looking forward to being able to provide our affiliate partners with improved tracking functionality on both desktop and mobile devices, and also giving them a greater level of reporting, enabling them to optimise their campaigns more comprehensively,"

- Allan Turner, Head of Performance at BGO Entertainment

Also of interest, the day of this re-launch, February 26, coincides perfectly with a sudden and drastic flood of unsolicited marketing messages hitting U.K. mobile subscribers[54]. An example of the messages sent is shown to the right.

```
You can win real money from your sofa! 20 FREE spins, no deposit reqd. Start winning now at http://klck.co/9BV6K8 . 2STOPMSGSRP-LY'OUT' / unsb.me
```

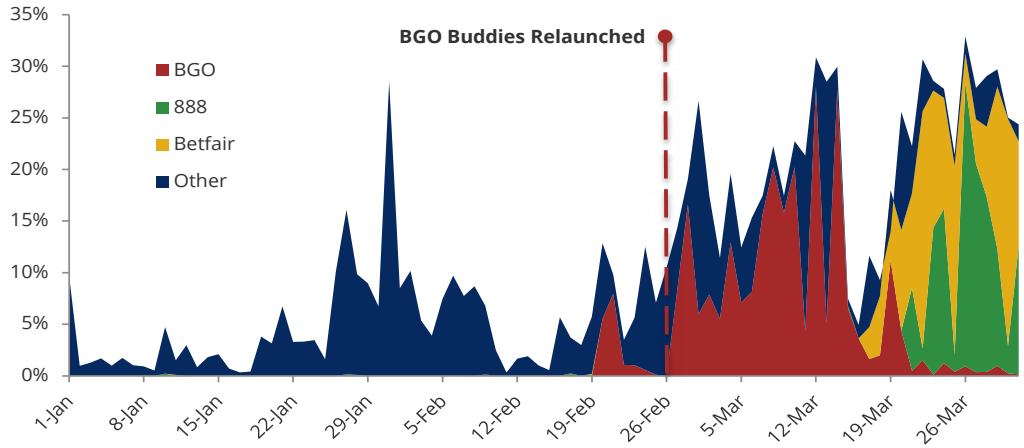

Fig. 6: *Casino Ads' Percentages of All Reported U.K. SMS, 15Q1*

```
Want to try any of our exciting slots and games, for FREE with 88 at 888 casino? http://klck.co/9EKNGU 18+T&Cs 2STOPMSGSRP-LY'OUT' / unsb.me
```

It's apparent from reports to the U.K. Spam Reporting Service that at least one affiliate was excited by BGO's new offerings and possible revenue. Rather than the typical mass marketing path of email and website ads, this affiliate took to blasting via SMS. At its peaks, this campaign was accounting for 15 to 25 percent of all reported mobile messages in the U.K. each day. Just a few weeks later in mid-March, this campaign almost disappeared.

Each message's formulaic nature even across campaigns makes it apparent that these were from the same source. The timing of these campaigns, while possibly coincidental, also suggests that it was not just multiple, unrelated affiliates or companies using the same messaging platform. These attempts continued through the few remaining weeks of the quarter, perching casino ad campaign volumes at 10 percent of all U.K mobile reports.

```
Want 5 totally FREE to spend on our massive range of exciting real money games at Bet-fair Casino? http://klck.co/9D3J37 18+T&Cs 2STOPMSGSRPLY'OUT' / unsb.me
```

[54] http://www.igamingbusiness.com/news/bgo-re-launches-affiliate-programme-income-access

Compromised Routers and other CPE

Customer-premises equipment also known as customer-provided equipment (CPE) has been the target of security research for some years now. These devices include routers, DSL/cable integrated networking adapters and Internet gateways that sit on the customer's premises and allow connections to the various telecommunication media. Unfortunately, these ubiquitous devices are increasingly becoming a core problem for both consumer and Internet security.

Low Hanging Fruit

A plethora of low hanging fruits exist in the form of vulnerabilities in CPE that make for a both an easy and effective target. One of the easiest attacks consists of scanning the Internet for devices still configured with their default login credentials. Many of these devices come out of the box with a predefined user name and password that can be found easily on various websites, given the make or model. Alternatively, a list of these default passwords makes brute-force guessing the login to many devices a trivial exercise. Various tools and sites such as SHODAN exist for easily discovering and scanning Internet-facing devices. The ability to find these vulnerable devices in a simple way allows for malicious mass login attempts using default credentials. Security researcher Kyle Lovett estimates that roughly 25 to 80 million of CPE devices in small and home offices are still configured with default credentials that leave them vulnerable.[55]

Just as default credentials have been around for ages, serious flaws in the basic firmware in many of these devices have been published publicly for years. Unfortunately, once installed, CPE devices are rarely updated with firmware patches so they tend to remain vulnerable even if a fix is available from the manufacturer. Over a million ADSL routers issued by 14 vendors were found to have outdated firmware from 2007. This firmware is known to have various critical vulnerabilities that can grant any attacker full control over the device.

One such example of a known flaw that persists to this day is known as "directory traversal." This vulnerability allows anyone, even the unauthenticated, to probe the device for information about how it is configured. This includes an encrypted hash of the admin credentials that is often times too weak to prevent hackers from decrypting it. Discovered as far back as 2011, this vulnerability is still seen in unpatched firmware to this day. The flawed and unpatched firmware responsible seen by Lovett was being still used on at least 700,000 ADSL routers given to customers around the world by their ISPs.

Another innocuous preset that leaves many endpoints vulnerable to compromise is due to the

[55] http://www.computerweekly.com/news/2240242736/Home-devices-threaten-enterprise-data-security-warn-researchers

issuing ISP. Many ISPs configure their consumer devices to enable and accept remote management by default for support purposes. However, nearly 60 percent of the ADSLs scanned by Lovett were easy-to-compromise devices that had hidden support accounts with the same easily guessable password.

The Difficulty of Securing CPE

These issues tend to have a larger impact on developing telecommunication markets due to the difficulty of meeting the demand of rapid growth. Security and up-to-date firmware are rarely, if ever, a profit driving focus in a market that already struggles with slim margins. These poorly secured CPE devices were found in Colombia, India, Argentina, Thailand, Moldova, Iran, Peru, Chile, Egypt, China and Italy according to Lovett. Others in countries such as the U.S. appear to be off-the-shelf routers purchased by consumers rather than distributed by the ISP.[56]

Automatic updates similar to desktop operating systems may seem like an easy solution, but these services could bring more issues. Currently, many ISPs remotely reconfigure and upgrade the software on home routers using a protocol called TR-069. Shahar Tal, a security researcher, did some digging on this protocol and found that less than 20 percent of the deployed endpoints found used SSL and many failed to properly verify certificates.[57] On the ISPs side, the management servers responsible for issuing the commands via TR-069 were not much better. Shahar Tal found remote code execution vulnerabilities within days of analyzing two open source offerings, while a widely adopted commercial version was vulnerable to SQL injection attacks.

Malicious Uses of a Compromised CPE

Compromised devices are often used for three purposes: DNS redirection, finding more easy-to-compromise devices, and distributed denial of service (DDoS) attacks.

By controlling the victim's DNS settings, attackers can redirect or even hijack portions of their Internet traffic. For example, an attacker could redirect URLs to any IP they wanted to serve malware or ads, inject ads into other sites, poison search results such as how to remove said compromises, or man-in-the-middle traffic to hijack a log in. Also, these are not limited to a certain operating system or desktop machines. For example, a mobile phone, tablet, or any other device connected to a compromised router is just as vulnerable to having it's traffic redirected or hijacked.

Compromised routers are also used for more than just redirecting the victim's computer traffic to malicious sites. Often times these routers are setup as zombie members of botnets that remotely control the routers' actions via central Command and Control servers (CnCs.) This centralized control is then often times used to dole out targets for the compromised routers to scan for vulnerabilities.

[56] http://www.computerweekly.com/news/2240242736/Home-devices-threaten-enterprise-data-security-warn-researchers
[57] http://shahart.al/I-hunt-TR-069-admins-shahar-tal-dc22.pdf

Thus, these hacked routers give attackers a vast number of free resources with which to find and compromise even more poorly secured devices — compounding the problem. Since the devices are owned by legitimate users who are spread across the world, blocking or fixing the compromised routers is difficult.

It's also common for the wranglers of these botnets to use this large, geographically diverse set of hacked routers to launch DDoS attacks against targets on the web. Currently, a very famous example of this is that of Lizard Squad using a botnet of home routers to carry out attacks on Microsoft's Xbox Live and Sony's Playstation Network, among other targets.

Lizard Squad's DDoS service, LizardStresser, coordinates and controls compromised routers[58] in mass to use SYN floods, UDP floods, DNS amplification via open resolvers, or a combination of these to cripple their chosen targets. Hacked CPE devices can also be configured to function as recursive open DNS resolvers, as well — thus allowing the botmasters to create their own functionality for amplification attacks from scratch. The malware used to control the compromised devices can infect various versions and flavors of Linux, MIPS, SPARC-servers and other devices such as routers. This gives the group a wide variety of choices for what can be viable to compromise when searching for weakly secured CPE devices. Unfortunately, these security problems still impact those with secure CPE devices. Lizard Squad now offers this service for just $5.99 a month to knock targets offline for 100 seconds.

Avoiding and preventing these types of issues is a multifaceted problem that requires better scrutiny of the device manufacturers, the router vendors, and ISPs delivering these devices to households. This list of flaws stem from each of the various points in this chain making the solution less than straightforward. However, it's clear that there should be a robust and secure way to push firmware updates to these devices, and that any device that does not support this should come with an expiry date, because vulnerabilities will almost certainly be found within a year or two of shipping.

[58] http://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/

DNSSEC History

The Domain Name System (DNS) was originally defined as a hierarchical directory-like system intended to provide human-readable host name to IP resolution services in a manner that supports distributed delegation of sub-nodes. This distributed service evolved quickly and became critical to the functioning of many systems connected to the Internet. The core protocol was defined with implied trust from upper levels of the directory and relies on a process of referrals for lookups.

An added DNS security layer has been a long-standing desire, to improve the level of trust that clients could place in DNS responses. A controversial fix was developed in 1994 under the name DNS Security Extensions (DNSSEC). DNSSEC enabled resolvers to validate each response received in the DNS tree by cryptographically verifying keys published from the top level of the directory and down. Due to its complexity and debatable value, discussion around the solution dissipated. Debate around the deployment of DNSSEC was reignited in 2008 when researcher Dan Kaminsky discovered a potent flaw that allowed attackers to poison the results from vulnerable DNS servers.[59]

DNSSEC Benefits

Through a series of new DNS record types and a cryptographic validation process, DNSSEC enables authentication of DNS responses from the top DNS directory hierarchy down to the end DNS node, and is intended to provide the DNS client with assurance that the DNS response received from a domain name server was not manipulated by a third party in transit. By cryptographically validating each DNS response, the recursive resolver can significantly reduce the possibility that a MITM attempting a cache poisoning attack can successfully return a modified DNS result which the recursive resolver would then store in its cache, preventing malicious traffic redirection for the period of time that the entry would have been otherwise cached.

From the end user perspective, the use of DNSSEC should be imperceptible. The DNSSEC protocol was designed to be backwards compatible with the legacy DNS protocol to enable a smooth transition for legacy systems leveraging DNS. DNS stub resolvers who wish to leverage DNSSEC issue DNS requests with a specific flag set, requesting that the recursive resolver carry our DNSSEC validation of any returned results for a given resource. Only in the case that DNSSEC validation fails, due to misconfiguration or operational issue for a given domain, will the user see an difference in behavior. In the case that a non-DNSSEC aware client initiated the query, they would receive results regardless of the DNSSEC problem. In contrast, DNSSEC-aware clients would likely receive a DNS error and no results from their lookup.[60]

[59] http://www.theregister.co.uk/2008/07/24/dns_exploit_goes_wild/
[60] http://www.internetsociety.org/deploy360/blog/2015/03/hbo-now-dnssec-misconfiguration-makes-site-unavailable-from-comcast-networks-fixed-now/

DNSSEC Challenges

One of the major roadblocks facing DNSSEC's widespread adoption is the difficulty of deployment and management. Several base-level requirements must first be met:

- Your domain's top-level domain (TLD) needs to support DNSSEC.
- The domain's registrar must support Delegation Signer (DS) records.
- Your DNS server software and DNS hosting provider must support DNSSEC.

Regarding the first requirement, each domain's TLD zone must be signed and that domain's signing record zone must be added to the "." (root) zone. As of March 2015, only 79 percent of all TLDs and ccTLDs support DNSSEC.

In order for a domain's DS key to be added to the root zone for the domain's TLD, the domain registrar must support a mechanism for the configuration of DS records within their management tools and they must be able to communicate these DS records to your domain's top-level domain.

Thirdly, the various tools and processes for signing zones are challenging to understand and are missing the needed automation frameworks for zone management and re-signing, leading to added administrative overhead. Signed zones also need to be re-signed after every update and on an ongoing short interval basis. These signing events can be especially problematic for zones with a large volume of entries as these zones may require a long time to sign.

Once launched, other issues come into play as well. When the DNSSEC signing process breaks anywhere within the DNS hierarchy, signed domains can effectively appear to be "knocked offline" from the client perspective until the problem is first fixed and then standing TTLs expire on remote DNS servers. Even those well versed in the technology have had hiccups. OpenDNSSEC, an open-source project aimed at creating a turn-key solution for using DNSSEC, has had management difficulties with their DNSSEC records. On January 25th, opendnssec.org suffered from a 12-hour outage due to allowing the domain's RRSIGs to expire.[61]

The load on both the authoritative and recursive resolver DNS infrastructure increases with DNSSEC and may require that network operators deploy more DNS infrastructure in order to support the functionality and the added transaction time can be perceptible to the end user.[62] Further, DNSSEC validation requires additional processing power on DNS resolvers to validate records via public key cryptography. DNS query response sizes will increase, as DNSSEC-compliant client queries will result in three to four times the current query response count, with the addition of DNSKEY, RRSIG and DS records. The volume of data in query responses will also increase significantly. One reason for this is because the RRSIG record that provides signing information for every DNS record is

[61] http://ianix.com/pub/dnssec-outages/20150125-opendnssec.org/
[62] http://www.potaroo.net/ispcol/2014-08/dnsseccost.html

typically much larger than the standard record. For example, the MX query response for Comcast is six times smaller with DNSSEC disabled:

```
$ dig MX comcast.net
…
;; MSG SIZE rcvd: 394
```

Example MX query response with DNSSEC enabled returns 2457 bytes:

```
$ dig MX comcast.net +dnssec
…
;; MSG SIZE rcvd: 2457
```

Lastly, some DNS concepts are not compatible with DNSSEC. Wildcard records are not supported, so the signed record for "*.example.com" would not be able to be DNSSEC-authenticated when "www.example.com" is queried.

DNSSEC and Security

Beyond the issues of deploying and maintaining DNSSEC, concerns have also arisen that it may in some cases enable new attacks or reduce security.

For instance, the large DNS responses associated with DNSSEC enables abuse via DNS amplification or reflection attacks. By design, DNS leverages the connectionless UDP protocol and this enables source address spoofing of specifically crafted DNS requests that are known to return very large DNS responses. The ratio of response data size to the original request data size can be upwards of 50 to one. By leveraging this spoofing technique, an attacker can leverage a large network of openly accessible DNS resolvers and very limited source bandwidth to generate a flood of DNS responses at their intended target, overwhelming the target system and the target's network provider with 100's of gigabits of traffic per second.

By design, DNSSEC asserts the existence of a record in addition to the non-existence of records. Between real record entries are swathes of non-existent entries DNSSEC must assert as not existing of via a special DNS record type, "Next Secure" (NSEC). The purpose of NSEC records is to disclose what the next signed entry in a zone file is so that all other records in between one record and the next can be declared non-existent. This DNSSEC characteristic allows an attacker to quickly compile the full list of existing DNS entries in a zone, enabling enumeration of the various systems specified within a given zone file.

Previously, the ability to view complete zone files was gated by obscurity. The contents of a zone would need to be generated via automated guesswork. The NSEC records are an easy way to find targets for the delivery of email spam and for planning future network attacks. The NSEC3 record provides a partial solution to this by only supplying hashed responses for validating the next domain name, but deploying NSEC3-compatible zones comes with the downside of additional management overhead.[63]

[63] http://www.links.org/dnssec/draft-ietf-dnsext-nsec3-00.html

Whether domain owners believe DNSSEC is worthwhile or a waste of time it has yet to reach widespread adoption. This is especially apparent when looking at the number of DNSSEC-signed domains in the top TLDs. The adoption of DNSSEC by domains registered within these top TLDs remains extremely low.[64]

The Future of DNSSEC

Certain new and proposed Internet protocol standards seek to leverage the DNSSEC chain of validation model to enhance network service security such as DNS-Based Authentication of Named Entities (DANE).[65] DANE aims to improve the security of various network services by enabling service owners to specify that a) a service should always be connected to via TLS and b) that a specific CA or end entity certificate should be expected when making a connection. DANE seeks to deemphasize the need for public certificate authorities (CA) that are intended in the pre-DANE world to be equally trustworthy and able to generate certificates for any host name. In practice, this utopian view of universal CA trustworthiness is fraught with frequent examples of errors and abuse,[66, 67] and this is something that DANE has the capability to improve upon. For example, a proposed standard that leverages DANE for the Simple Mail Transfer Protocol (SMTP) seeks to extend DANE validation for SMTP client to SMTP server connections,[68] closing several longstanding loopholes that could prevent secure email delivery.

The jury is still out on whether DNSSEC will ever reach broad adoption. Early adopters have typically been governmental organizations and financial institutions, along with specific regional pockets of network operator enthusiasm. However, some of the world's largest network operators have so far found DNSSEC deployment and management to be too onerous to undertake. A mix of new potential uses, the known deployment challenges, and continued questions regarding the security and utility of DNSSEC will factor in to the potential deployment plans of network managers.

[64] http://www.statdns.com/
[65] RFC 6698, https://tools.ietf.org/html/rfc6698
[66] http://www.computerworld.com/article/2486614/security0/french-intermediate-certificate-authority-issues-rogue-certs-for-google-domains.html
[67] http://googleonlinesecurity.blogspot.com/2015/03/maintaining-digital-certificate-security.html
[68] https://datatracker.ietf.org/doc/draft-ietf-dane-smtp-with-dane/

About Cloudmark

Cloudmark provides intelligent network security solutions that protect organizations' most valuable resources and defend against security breaches that result in revenue loss, increased costs and brand damage. Only Cloudmark combines predictive global threat intelligence from hundreds of service providers and thousands of enterprises with real-time defense and cross-vector correlation, including messaging and DNS, in a software solution that deploys rapidly to safeguard organizations and detect attacks before they happen. Cloudmark protects more than 120 tier-one service providers and 70,000 enterprise customers through partners, including Cisco, McAfee, and Microsoft. Key customers include AT&T, Verizon, Swisscom, Comcast, Cox, NTT and more than 1 billion subscribers worldwide.

Americas Headquarters
Cloudmark, Inc.
San Francisco, USA

Europe
Cloudmark Europe Ltd.
London, UK

Paris
Cloudmark Labs
Paris, France

Japan
Cloudmark Japan
Tokyo, Japan

CLOUDMARK®
Intelligent Network Security

www.cloudmark.com