

SPAMCHANNEL

SPOOFING EMAILS FROM +2 MILLION DOMAINS AND VIRTUALLY
BECOMING SATAN



WHOAMI

- Marcello Salvati (@byt3bl33d3r)
 - Same handle on Twitter/Mastadon/BlueSky, Github, LinkedIn
- FOSS Developer, Researcher, “Infinity Stones” Teamer (I collected all the colors)
 - 10+ years
- Hiring? Let’s talk!



DISCLAIMER

Don't do crimes plz 🙏

Like for realz.

I'm not responsible if you do, you'll get in trouble.



I JUST WANTED TO SEND AN EMAIL ... PROGRAMMATICALLY ... THROUGH A CLOUDFLARE WORKER

FOR THE UNINITIATED...

<https://workers.cloudflare.com/>



Edgy Serverless computing

Think emo AWS lambdas. Only in Javascript/TypeScript/WASM

CF WORKERS IOI

1. `npm create cloudflare@latest`
2. Create `worker.js`
3. `npx wrangler deploy`
4. You're worker is available at
`https://<YOUR_WORKER>.<YOUR_SUBDOMAIN>.workers.dev !`

```
export default {  
  async fetch(request, env, ctx) {  
    return new Response('Hello World!');  
  },  
};
```

<https://developers.cloudflare.com/workers/get-started/guide/>

LUCKY ME!

Send email using Workers with MailChannels

05/13/2022



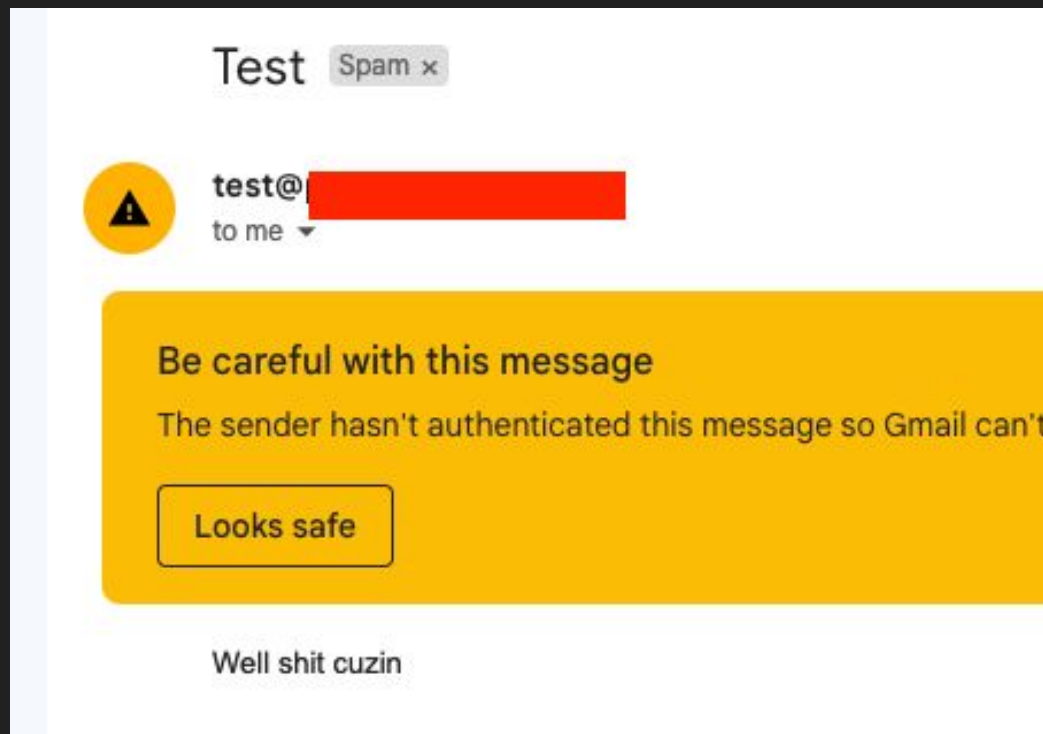
Erwin van der Koogh



<https://blog.cloudflare.com/sending-email-from-workers-with-mailchannels/>

```
export default {
  async fetch(request) {
    send_request = new Request('https://api.mailchannels.net/tx/v1/send', {
      method: 'POST',
      headers: {
        'content-type': 'application/json',
      },
      body: JSON.stringify({
        personalizations: [
          {
            to: [{ email: 'test@example.com', name: 'Test Recipient' }],
          },
        ],
        from: {
          email: 'sender@example.com',
          name: 'Workers - MailChannels integration',
        },
        subject: 'Look! No servers',
        content: [
          {
            type: 'text/plain',
            value: 'And no email service accounts and all for free too!',
          },
        ],
      })
    })
  }
}
```

<https://blog.cloudflare.com/sending-email-from-workers-with-mailchannels/>





**SOME TIME
LATER**



mkuchak

May '22

So basically, does this allow other developers using Workers to impersonate me and send emails from my domains (if I add [SPF](#) ⁷ records)?

Any way to prevent third parties from sending emails on my behalf?



ksimpson

May '22

The sad truth is that anyone can impersonate your domain right now from a whole variety of services on the Internet. To protect yourself, we highly recommend setting up and properly using DMARC so that receivers know that email from your domain has to be signed and that it must come from only authorized sources.

The Messaging, Malware, Mobile Anti-Abuse Working Group (M3AAWG) recently published some guidelines on how to best protect your domain online. It's a free download and is packed with information that will be useful to you: https://www.m3aawg.org/sites/default/files/m3aawgbrandprotectionkit_domainmanagement.pdf ²⁷

▲ [-] Keavon 5 points 1 year ago ▼

What's the catch? Free, with no monetization at all? Surely there are at least limits? I'd love more information about that.

[permalink](#) [embed](#) [save](#) [report](#) [give award](#) [reply](#)

▲ [-] ttul 4 points 1 year ago ▼

I work at MailChannels. We are the largest transactional mail sender on the internet in terms of domains and individual senders, because we send email for hosting companies. Spammers constantly try to send through hacked Wordpress sites and such, and blocking that stuff is our reason for existing. We are very good at it.

So if there is a catch with the Cloudflare integration, it's that we don't have a very high tolerance for silly business. If we notice badness, you will be limited or blocked.

LITERALLY....



HOL UP A MIN...

```
export default {  
  async fetch(request) {  
    send_request = new Request('https://api.mailchannels.net/tx/v1/send', {  
      method: 'POST',  
      headers: {  
        'content-type': 'application/json',  
      },  
      body: JSON.stringify({  
        personalizations: [  
          {  
            to: [{ email: 'test@example.com', name: 'Test Recipient' }],  
          },  
        ],  
        from: {  
          email: 'sender@example.com',  
          name: 'Workers - MailChannels integration',  
        },  
        subject: 'Look! No servers',  
        content: [  
          {  
            type: 'text/plain',  
            value: 'And no email service accounts and all for free too!',  
          },  
        ],  
      })),  
  },  
}
```

MAILCHANNELS + CLOUDFLARE PARTNERSHIP

MailChannels created a “Transactional API” (TX API)

- <https://api.mailchannels.net/tx/v1/documentation>
- No auth required
- Allowlisted to Cloudflare IPs

TL;DR: Anyone with a Cloudflare account can send emails through MailChannels!

<https://blog.cloudflare.com/sending-email-from-workers-with-mailchannels/>

MAILCHANNELS + CLOUDFLARE PARTNERSHIP

1. Create a Cloudflare account (Free)
2. Upload a Cloudflare Worker that sends HTTP POST to MailChannels TX API with Email details
3. Email sent through MailChannels
4. Profit????!????!!???



IhsanGans

Jun '22

I've updated my previous code in gist [Send email from Workers with MailChannel API · GitHub](#) 66

You can try it now here [Submit your email](#) 31

Shout out to @ihsangan

<https://gist.github.com/ihsangan/6111b59b9a7b022b5897d28d8454ad8d>

Marcello Salvati @byt3b133d3r

Submit your email

← → ↺ 🔒

(*) is required

sender@example.com *

Sender Name

receiver@example.com

Receiver Name

reply-to@example.com

Replier Name

DKIM Domain

DKIM Selector

DKIM Private Key
MIICXQIBAAKBgQCU.....

Plain ▾

Email Subject *

Email Body *

submit

TEST CASE I - A DOMAIN THAT DOESN'T EXIST

Sender: test@wattahogger.com

```
{"errors":["Failed to send email: 550 5.1.2 [SDNF] Sender  
Domain Not Found.  
https://console.mailchannels.net/insights/bounce?  
auid=cloudflare\u0026sender=test%40wattahogger.com\u0026txid=1  
f57aafe78bbf25d"]} }
```

TEST CASE 2 - A DOMAIN THAT EXISTS

Sender: test@example.com

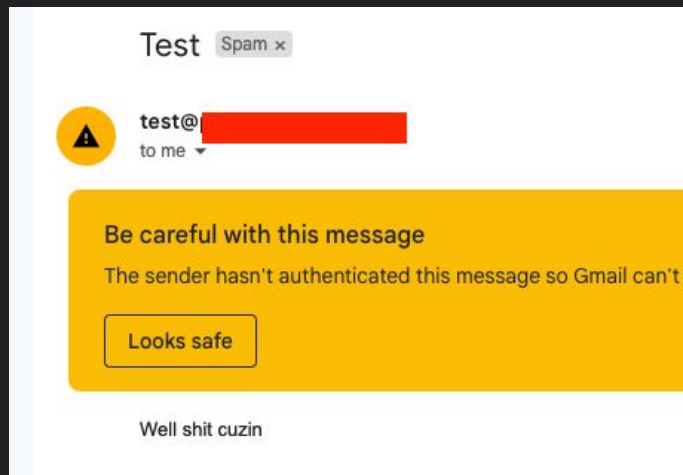


null

???? yay?

TEST CASE 2 - A DOMAIN THAT EXISTS

Sender: test@example.com



To:	deezeggnogs@gmail.com
Subject:	Test
SPF:	SOFTFAIL with IP 23.83.208.75 Learn more
DMARC:	'FAIL' Learn more

TEST CASE 3 - A DOMAIN THAT ACTUALLY USES MC

Google



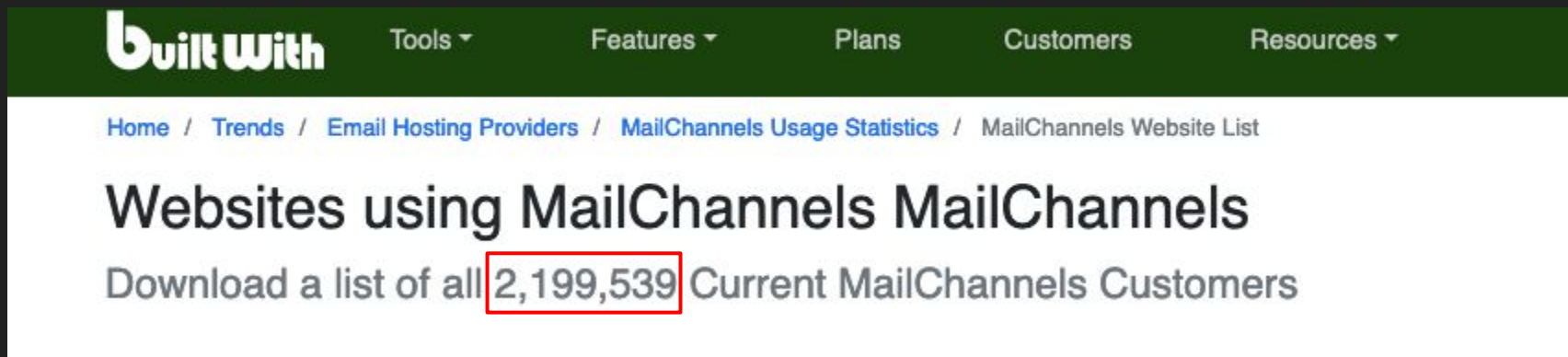
websites that use mailchannels



Google Search

I'm Feeling Lucky

FINDING A DOMAIN THAT USES MC



The screenshot shows the BuiltWith website interface. The top navigation bar is dark green with the 'builtwith' logo and links for Tools, Features, Plans, Customers, and Resources. Below the navigation bar, a breadcrumb trail reads: Home / Trends / Email Hosting Providers / MailChannels Usage Statistics / MailChannels Website List. The main heading is 'Websites using MailChannels MailChannels'. Below this, a text line states 'Download a list of all 2,199,539 Current MailChannels Customers', where the number '2,199,539' is highlighted with a red rectangular box.



<https://trends.builtwith.com/websitelist/MailChannels>

FINDING A DOMAIN THAT USES MC

Website	Location	Sales Revenue	Tech Spend	Social	Employees	Traffic
brainpop.com	United States		\$10000+	10,000+		High
lto.comed.com	United States	\$411k+	\$5000+	10,000+		Medium
timesfreepress.com	United States		\$2000+	20,000+		High
calguns.net			\$100+			Medium
bicyclecards.com	United States	\$124k+	\$2000+	5,000+		Medium
native-languages.org			\$100+			High
thewarmingstore.com	United States	\$84k+	\$2000+	2,000+		Medium
travelmamas.com	Canada		\$100+	10,000+		High
cinemawest.com	United States		\$250+			-
tnlottery.com	United States		\$100+	2,000+		-
totallyfurniture.com	United States	\$351k+	\$50+			High
batteryjunction.com	United States	\$87k+	\$2000+	500+		Medium
carandtruckremotes.com	United States	\$26k+	\$1000+			-
boston.gov	United States	\$536k+	\$5000+			High
cordcuttingreport.com			\$100+	10+		Medium
onlinestatbook.com			\$50+			Medium
commonsensehome.com	United States	\$53k+	\$250+	1,000+		Medium
lrc.cod.edu	United States		\$5000+	250+		High
notepad-plus-plus.org			\$50+	5,000+		Very High
tcrf.net			\$50+			Medium
behringer.com	United States		\$50+	20,000+	1,000+	High

Report Suggestions

The more relevant a list the more chances of converting leads.

All sites that have ever used MailChannels

Websites currently and historically using MailChannels.

MailChannels websites with estimated Sales Revenue over \$1m

MailChannels websites with estimated Sales Revenue over \$1m.





















MailChannels websites with estimated Sales Revenue over \$100k

MailChannels websites with estimated Sales Revenue over \$100k.

<https://trends.builtwith.com/websitelist/MailChannels>

FINDING A DOMAIN THAT USES MC

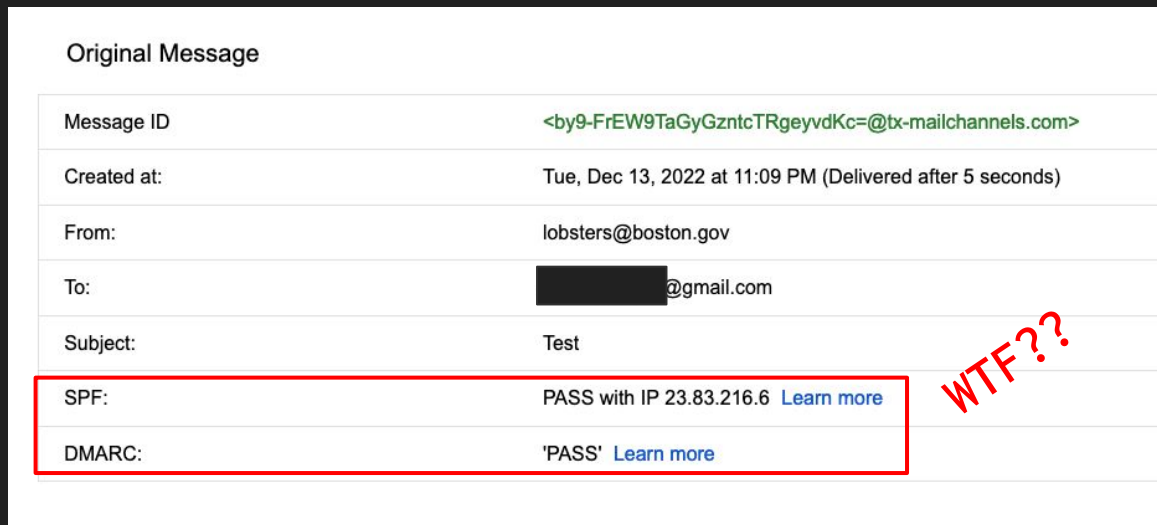
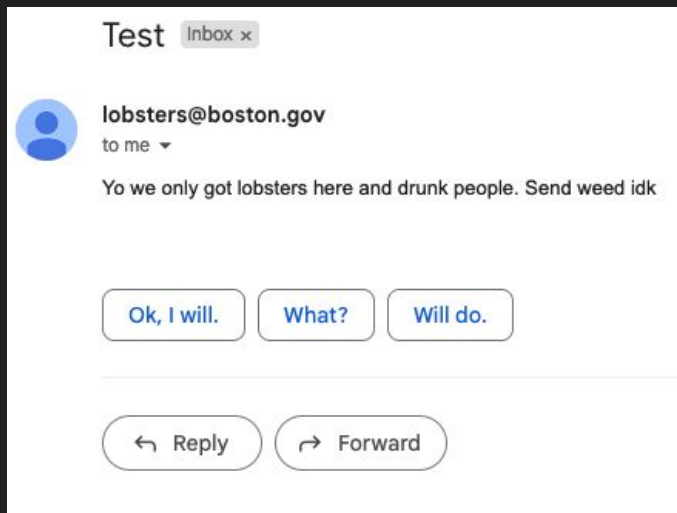
Trusted by leading service providers:

 WPengine	 DreamHost	 HOSTINGER	 HostPapa	 KINSTA
 locaweb	 enom	 1-grid <small>GET ONLINE WITH US</small>	 ptisp	 o2switch
 dewaweb	 Rebel	 turbify	 arvixe <small>web hosting</small>	 site5
 a small orange <small>business hosting</small>	 Hostwinds <small>DESIGN IN YOUR HAND</small>	 webafrica	 GreenGeeks <small>WEB HOSTING</small>	 WOWRACK

<https://www.mailchannels.com/customers/>

TEST CASE 3 - A DOMAIN THAT ACTUALLY USES MC

Sender: lobsters@boston.gov



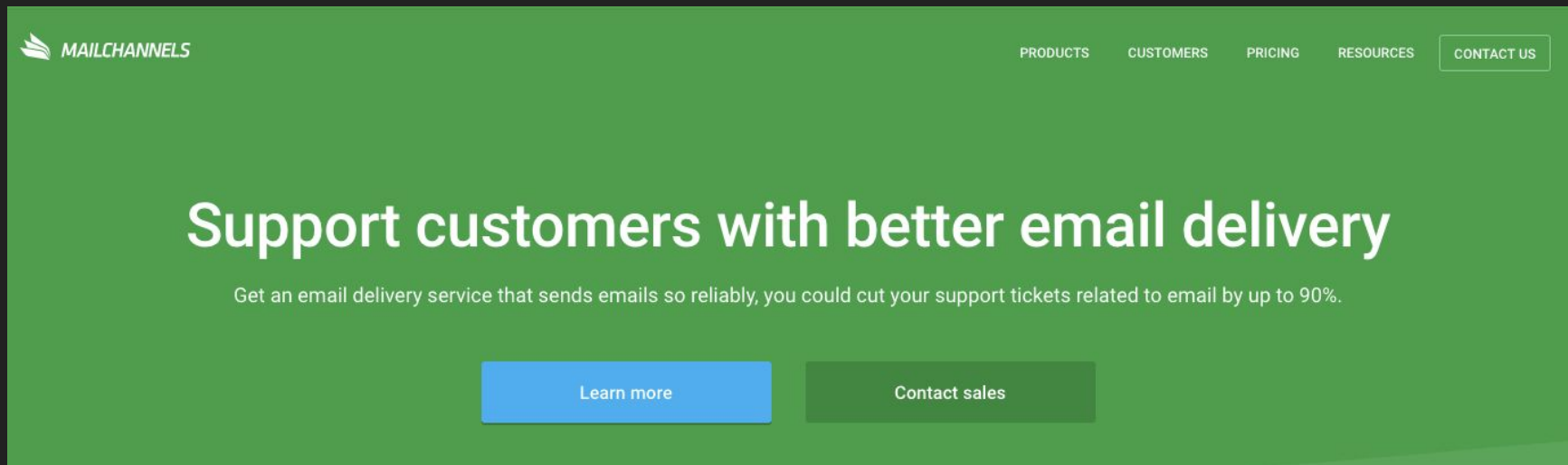
TEST CASE 3 - A DOMAIN THAT ACTUALLY USES MC


Sender: minus@notepad-plus-plus.org



HOL UP... WTF IS MAILCHANNELS?

MAILCHANNELS IS AN EMAIL TRANSACTION SERVICE

The image shows the top portion of the MailChannels website. The header is green with the MailChannels logo on the left and navigation links (PRODUCTS, CUSTOMERS, PRICING, RESOURCES, and a highlighted CONTACT US button) on the right. Below the header is a large green hero section with the headline 'Support customers with better email delivery' and a sub-headline stating that the service can reduce support tickets by up to 90%. At the bottom of the hero section are two buttons: 'Learn more' in blue and 'Contact sales' in green.

 MAILCHANNELS

PRODUCTS CUSTOMERS PRICING RESOURCES **CONTACT US**

Support customers with better email delivery

Get an email delivery service that sends emails so reliably, you could cut your support tickets related to email by up to 90%.

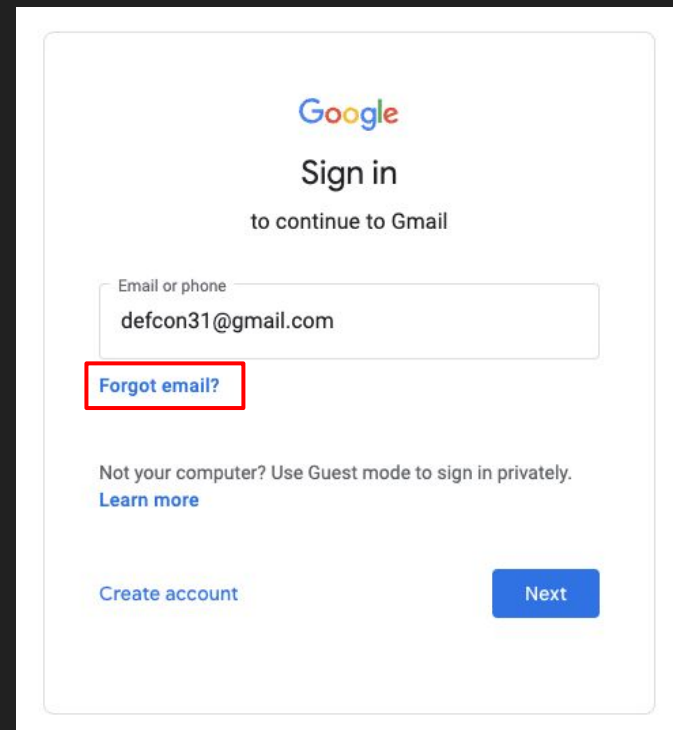
[Learn more](#) [Contact sales](#)

<https://www.mailchannels.com/>

EXAMPLES OF TRANSACTIONAL EMAILS

Automated emails (robot -> human)

- Password Resets
- Email Confirmations
- General Notifications
- Newsletters/Coupons/Promotions



The image shows a screenshot of the Google Sign-in page. At the top is the Google logo, followed by the text "Sign in" and "to continue to Gmail". Below this is a text input field labeled "Email or phone" containing the email address "defcon31@gmail.com". A red rectangular box highlights the link "Forgot email?" located directly beneath the input field. Further down, there is a line of text: "Not your computer? Use Guest mode to sign in privately." followed by a blue link "Learn more". At the bottom left is a blue link "Create account", and at the bottom right is a blue button labeled "Next".

SWEET SWEET IRONY...

Hackers exploit vulnerable web sites and user accounts to send spam and phishing emails



Spam damages your email reputation

Have you been blocked by Microsoft or Google? Outbound spam might be to blame



Email delivery problems cause tickets

25-50% of support tickets are caused by email delivery problems



Weak platform security breeds abuse

Is your hosting infrastructure well-protected against abuse? If not, you might become a haven for spammers

<https://www.mailchannels.com/>

#WeBlockSpam

THE MC DIMENSION

Comments



Khatamband

November 25, 2019 21:04

Comment actions ▾

it looks complex. Please do it for us. Here are login details

RDP

151.106.26.182

Administrator

Aarya**1212hii

Thanks

Ravi

Please [sign in](#) to leave a comment.

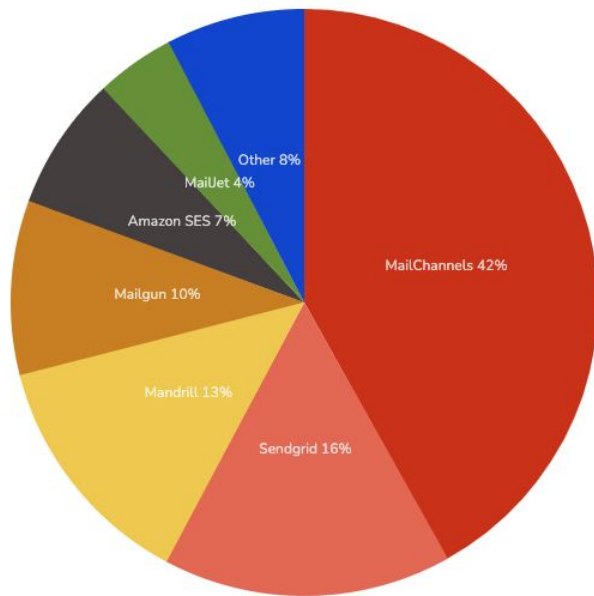
<https://support.mailchannels.com/hc/en-us/articles/200262550/comments/360004614572>

<http://archive.today/jcmCP>

WOAH

Transactional Email Usage Distribution on the Entire Internet

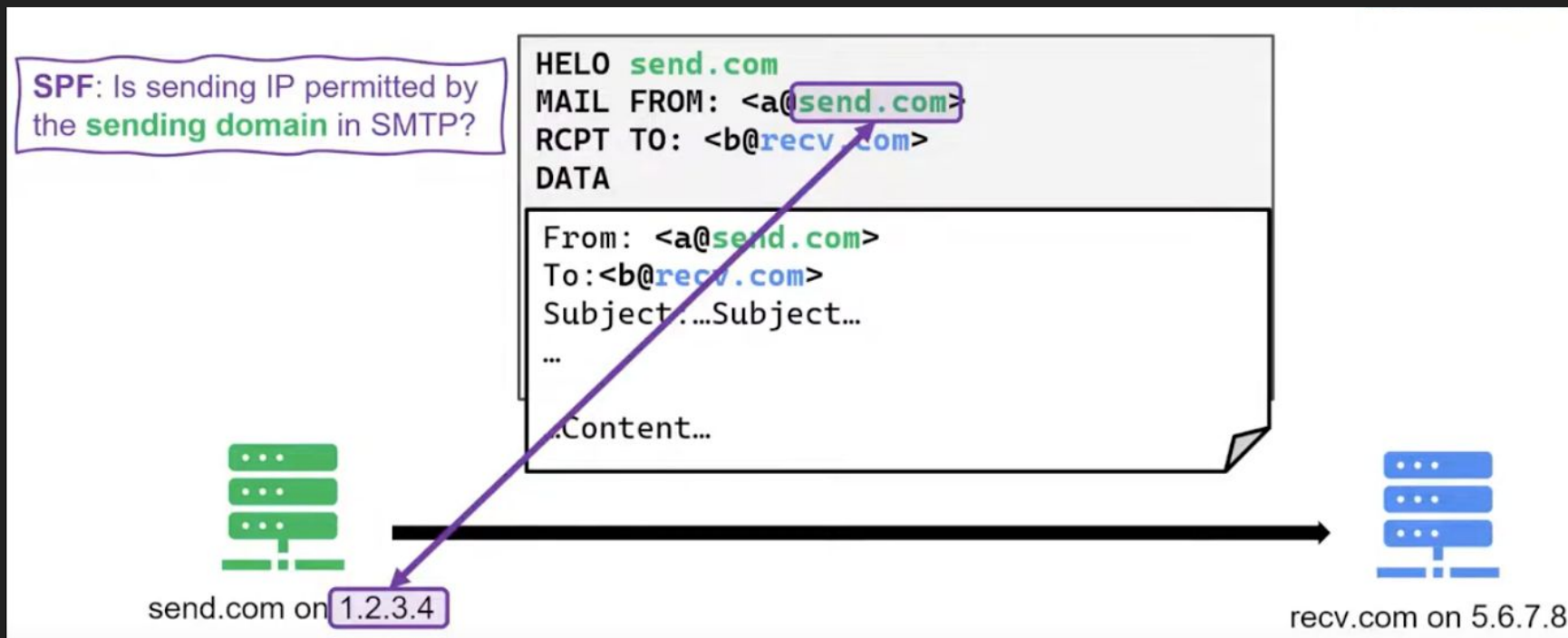
Statistics for websites using Transactional Email providers



Top In Transactional Email Usage Distribution on the Entire Internet

Technology	Websites	%
 MailChannels	2,199,539	1.02
 Sendgrid	834,254	0.39
 Mandrill	695,113	0.32
 Mailgun	504,241	0.23

SPF 101



<https://www.youtube.com/watch?v=V9kajr5dESs>

Chenkai Wang, Gang Wang // WWW'22 Talk: Revisiting Email Forwarding Security under the Authenticated Received Chain Protocol

MAILCHANNELS SPF RECORD

```
> dig TXT boston.gov
```

```
"v=spf1 ip4:140.241.0.0/16 ip4:35.170.24.210 ip4:63.101.151.0/28 ip4:18.205.196.151 ip4:205.201.128.0/20  
ip4:198.2.128.0/18 ip4:148.105.8.0/21 ip4:13.108.238.144 ip4:13.108.238.145 ip4:13.108.238.146  
ip4:13.108.238.147 ip4:13.108.238.148 " "ip4:13.108.238.149 ip4:13.108.238.150 ip4:13.108.238.151  
ip4:13.108.238.152 ip4:13.108.238.153 ip4:13.108.238.154 ip4:13.108.238.155 ip4:13.108.238.156  
ip4:13.108.238.157 ip4:13.108.238.158 ip4:13.108.238.159 ip4:107.20.210.250 include:_spf.google.com "  
"ip4:68.232.145.191/32 ip4:216.71.152.242/32 include:relay.mailchannels.net include:mail.zendesk.com  
include:spf-00241402.pphosted.com include:sfpd1.everbridge.net -all"
```

ROOT CAUSE ?

- All MC customers are instructed to add “include:relay.mailchannels.net” to their SPF record.
 - This permits MailChannels to send emails on behalf of their domain

CONSEQUENCES?

- All MC customers can spoof each other!
- MC is acting as an open relay when used through CF workers! We're guaranteed to pass SPF when spoofing a domain that uses MC!



08-02-2016, 10:26 AM

#1

AverageUser 
WHT Addict

Join Date: Sep 2009
Posts: 174

Is using relay.mailchannels.net etc. a security risk (email spoofing / fake SPF authentication)

More and more hosting services use outside email/email authentication servers like include:relay.mailchannels.net. But isn't it a security risk? Consider this scenario:

- Hosting_A.com uses mailchannels.net.
- Hosting_B.com uses mailchannels.net.

Hosting_A.com and Hosting_B.com are completely unrelated, separate services.

Obviously, customers want to have their email delivered, so on BOTH they include this in SPF:

include:relay.mailchannels.net

NOW - what if a spammer who is hosted on Hosting_B.com checks what domains are hosted on Hosting_A.com and then uses them to authenticate email and send spam? Since customers on Hosting_A.com authenticate relay.mailchannels.net and spammer can also authenticate relay.mailchannels.net, then he can spoof at spam customers from both Hosting_A.com and Hosting_B.com - BECAUSE they use the SAME SPF include?

Is it possible to prevent that?

<https://www.webhostingtalk.com/showthread.php?t=1588978>

08-02-2016, 03:21 PM

#2

mc-ken-simpson ◉
Junior Guru Wannabe

Join Date: Aug 2009
Location: Vancouver, Canada
Posts: 39

The scenario you describe is indeed possible. However the advantage of using MailChannels is that, if this happens to you, you can contact us and we will block the spammer.

Reply With Quote

1



<https://www.webhostingtalk.com/showthread.php?t=1588978>

FIRST CONTACT (Nov 2022)

Hi Marcello,

We don't provide DKIM signing of our customers' email traffic. They can sign messages themselves, in which case the signature will survive transmission through our environment since we don't modify message content or change existing headers.

We are aware that it's possible for anyone who sends email through our service to impersonate another domain that has authorized us in their SPF record to send email on their behalf. This is somewhat by design. We encourage customers to implement DKIM signing because SPF has this intrinsic vulnerability.

Is this essentially the vulnerability you have discovered?

Regards,
Ken

On Wed, Nov 30, 2022 at 5:23 PM 'Marcello' via Abuse <abuse@mailchannels.com> wrote:

Hello,

I've discovered what appears to be a vulnerability/misconfiguration that allows anyone without authentication to spoof emails from almost all Mailchannel customer domains. Is there a security contact i can forward the details too?

Thank you.

--

Ken Simpson
CEO, [MailChannels](#)

AM I DUMB DUMB??

Does this affect other similar services like Sendgrid, Mailgun etc.. ? TL;DR no!

- Sender Identity Verification
 - Similar to a Let's Encrypt Challenge
- Dedicated sending IPs
 - Allows you to set unique SPF's per customer
- Actual authentication on their API
 - API key ties account with verified domains. Restricts sending.

AM I DUMB DUMB??

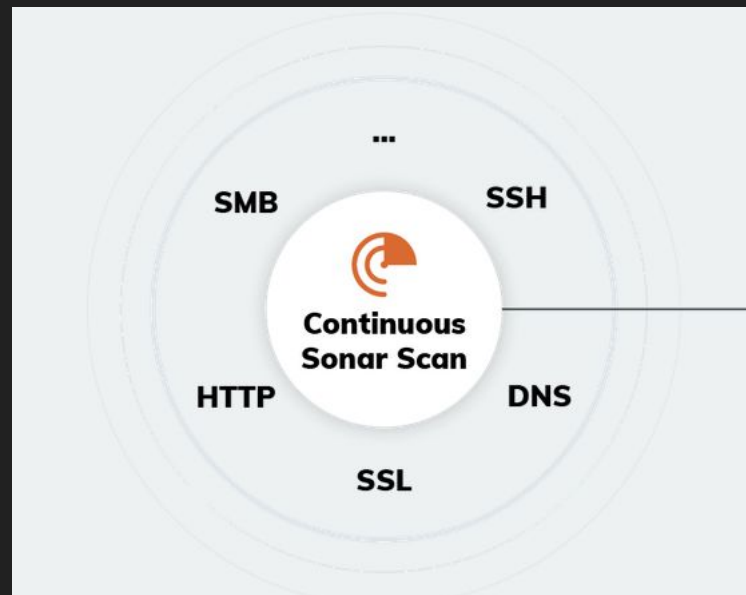
```
curl --request POST \  
  --url "https://api.sendgrid.com/v3/mail/send" \  
  --header "Authorization: Bearer $SENDGRID_API_KEY" \  
  --header 'Content-Type: application/json' \  
  --data '{"personalizations": [{"to": [{"email": "me@example.com"}]}, {"from": {"email":  
"ohmama@boston.gov"}, "subject": "Sending with SendGrid is Fun", "content": [{"type": "text/plain",  
"value": "and easy to do anywhere, even with cURL"}]}'  
  
{"errors":[{"message": "The from address does not match a verified Sender Identity. Mail cannot be sent  
until this error is resolved. Visit https://sendgrid.com/docs/for-developers/sending-email/sender-  
identity/ to see the Sender Identity requirements", "field": "from", "help": null}]}
```

TEAMING UP! RAPID7 & PROJECT SONAR

<https://www.rapid7.com/research/project-sonar/>

Huge shoutout to Rapid7 for helping out through all of this!

- Curt Barnard
- Matthew Kienow
- Tod Beardsley
- Spencer McIntyre
- Caitlin Condon



PROJECT SONAR SPF NUMBERS

- As of January 2023 according to Project Sonar
 - Domains with MailChannels SPF: 2207049

Builtwith.com is accurate!

SECOND REACH OUT (THIS TIME FROM RAPID7)

On Thu, Jan 5, 2023 at 4:42 PM Ken Simpson <ksimpson@mailchannels.com> wrote:

Hi Tod

We don't consider the SPF issue to be a vulnerability. By design, we do not restrict our customers to a particular set of sending domains on their account. Our customers are web hosting providers and they are not always in charge of the domains being used by their own end users. Therefore, it would be impossible for our customers to enumerate a set of permitted domains.

Domain owners are welcome to secure their domain against impersonation by signing messages with DKIM and setting up an appropriate DMARC policy, which will ensure that unsigned messages from an imposter will be rejected by receivers. DKIM signing and the use of DMARC is generally a good idea regardless of whether you are sending your email through a shared IP pool.

Regards

Ken

IT'S A FEATURE!

MailChannels main customers are web hosting providers who don't own the domains they send emails from!



HOW MAILCHANNELS DETECTS SPAM

- Signature checking against known spam signatures
- MaTh, StAtIsTiCs, TrEnDs
- IP/Domain reputation
- Analyzes email responses to gauge if receivers liked the email (?)
- Comparing previous emails from new ones via OCR (according to CEO)

<https://www.mailchannels.com/outbound/>

IN ALL OF OUR TESTING,
NONE OF OUR EMAILS WERE
BLOCKED...

ANALYZE THIS

“... Domain owners are welcome to secure their domain against impersonation by signing messages with DKIM and setting up an appropriate DMARC policy, which will ensure that unsigned messages from an imposter will be rejected by receivers...”



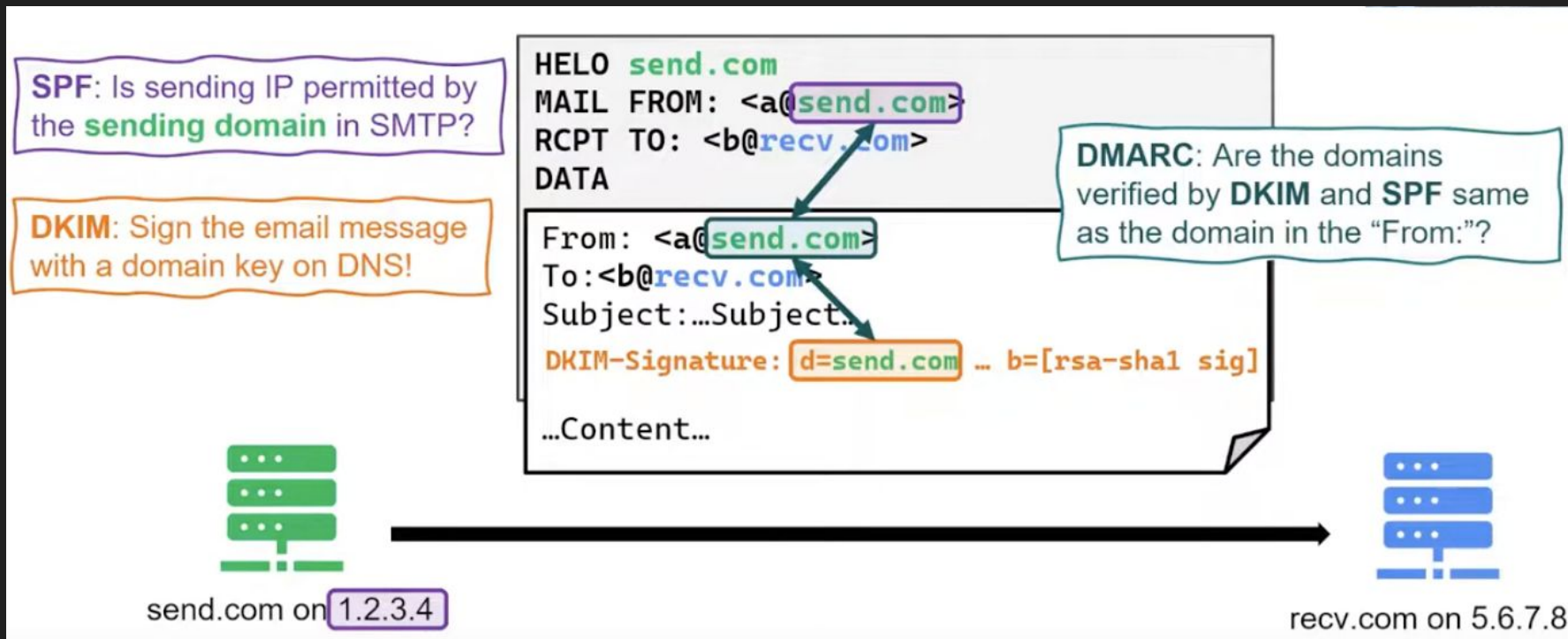
WASSUP WITH DMARC?

Remember we also passed DMARC...

Original Message	
Message ID	<by9-FrEW9TaGyGzntcTRgeyvdKc=@tx-mailchannels.com>
Created at:	Tue, Dec 13, 2022 at 11:09 PM (Delivered after 5 seconds)
From:	lobsters@boston.gov
To:	[REDACTED]@gmail.com
Subject:	Test
SPF:	PASS with IP 23.83.216.6 Learn more
DMARC:	'PASS' Learn more

WTF??

DMARC 101



<https://www.youtube.com/watch?v=V9kair5dESs>

PROJECT SONAR DMARC/DKIM NUMBERS

- January 2023, out of ~2M domains using MC:
 - Domains with any DMARC record: 407 (!)
 - Domains that use DKIM: 105 (!)



TEST CASE 4 - A DOMAIN THAT USES DMARC + DKIM

Gits.com - Seems serious about email!

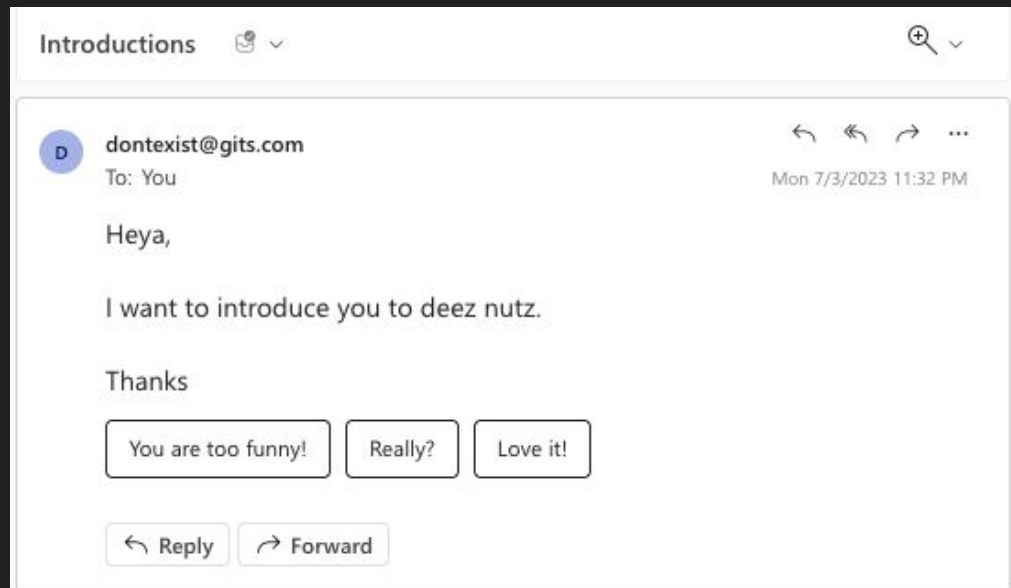
- SPF includes MC
- DMARC set to p=reject, sp=reject, adkim=s, aspf=s

```
> dig TXT _dmarc.gits.com
```

```
"v=DMARC1;p=reject;sp=reject;adkim=s;aspf=s;pct=100;fo=1;rf=afrf;ri=86400;  
rua=mailto:xfjwcenl@ag.dmarcian.com;ruf=mailto:xfjwcenl@fr.dmarcian.com"
```

TEST CASE 4 - A DOMAIN THAT USES DMARC + DKIM

Sender: dontexist@gits.com



... aaaand straight to
the inbox!

Does DMARC + DKIM HELP IN THIS SITUATION?

TL;DR no!

- We're guaranteed to pass SPF with MC (it's a feature)
- DMARC passes if SPF **OR** DKIM passes
 - Huge emphasis on the OR
- There's no proper way to tell receivers to strictly enforce DKIM!
 - In summary: You're also guaranteed to pass DMARC!



TEST CASE 4 - A DOMAIN THAT USES DMARC + DKIM



<https://www.mail-tester.com>

^ You're not fully authenticated -1

We check if the server you are sending from is authenticated

✓ [SPF] Your server 23.83.212.17 is authorized to use dontexist@gits.com	✓
✓ Your message is not signed with DKIM	-1
✓ Your message passed the DMARC test	✓
✓ Your server 23.83.212.17 is successfully associated with bird.elm.relay.mailchannels.net	✓
✓ Your domain name gits.com is assigned to a mail server.	✓
✓ Your hostname bird.elm.relay.mailchannels.net is assigned to a server.	✓

BUT WAIT....
THERE'S MORE!



WHAT'S THIS ARC-* STUFF?

Arc-Seal: i=1; s=arc-2022; d=mailchannels.net; t=1686606999; a=rsa-sha256; cv=none;
b=TC2r1PqesbE+yFb9k1m9UTgmCHEM++XitrPEkbnmS4d+BTt0J/GylUiJozewCfXUzWlWBm
xulvQLbGyw+MIQxL75sucLDYVsRQVRtw+FNFMNH/HEsZeigUQY+o0efKdIVX0CkcXeEKw
Uj5CarcIecs5bZw33tfyiMCsgSg6WxItYxaExbXBwIm0Yc9AvgTTqdjaJI9ssu6ZoW/2EH
H4bvSdQye7iTzs1WZw4T85lIDKhbANDrZm10jJ56SK883Z7GaUDNuuidxIT+Ww5DKMpZf1
5Q4H06iMQgz4mDiQnHqKNQh6Y/QC8W3RcBuHHfkYqcWkDUMdo9m0VbLKJEebZA==

Arc-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=mailchannels.net;
s=arc-2022; t=1686606999;
h=from:from:reply-to:subject:subject:date:date:message-id:message-id:
to:to:cc:mime-version:mime-version:content-type:content-type;
bh=YOK0VCVp7CzT11M4NZrS234v4IbihCvWbqzmvHtpwzY=;
b=uh0Xx5go8EgxzyXhvw9I/rkbmLY9AFS7xxmREJn9S10H33HNt4desH768PRuUg bjVaZ33k
KERoh1LTtA72aw2AEZVQjICBdYBxURX0/d/hok1lhzMkowj82ow+D0vgVsyRILBWI+rfJt
UcyFaEJs4kfgiqUzRgo7614Etjj8Mz686SkEuCEVT90mYECtil0VQogT+oBa6/3qz1/A7R
1Z7i06Lb8WUxncA/20ctigvcWcbVTGZq4IVnaeMnRMtSxFaw6NekN54dymrNfTcYDdFWfL
M9YxpTuccYVN2JN6+IPwM7WbiCfGrs5LznKdXPT8pWMPDe5IUwCLJalKnFN2kg==

Arc-Authentication-Results: i=1; rspamd=6c69b8658d-tt22k; auth=pass smtp.auth=cloudflare

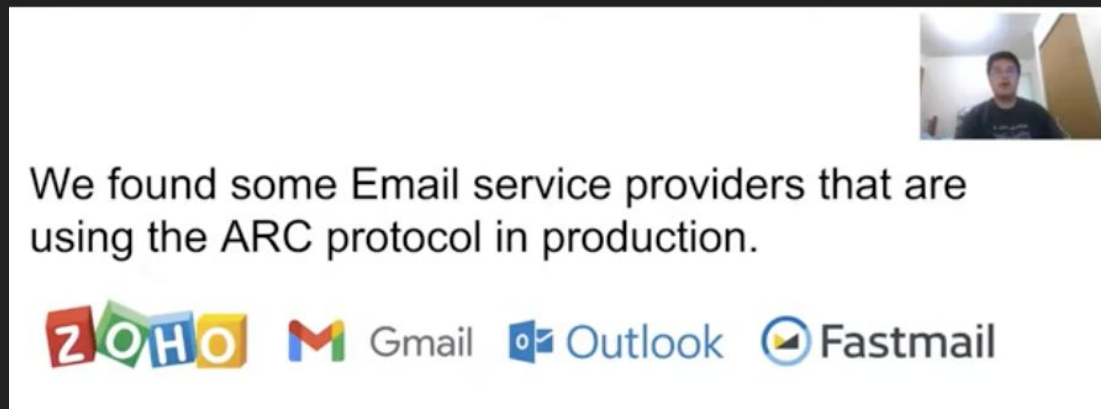
AUTHENTICATED RECEIVED CHAIN (ARC)

“...ARC allows an intermediate mail server to sign the message’s original authentication results so, that even when SPF or DKIM fails at the receiver end, the receiver can still check the chain of authentication records to determine whether the message can be accepted.. ”

- ARC was created to address the limitations of using existing email security extensions for email forwarding.
 - Couldn’t you just use DKIM? Yes. However, in reality using DKIM for email forwarding is impractical.
- RFC8617, Experimental (Published 2019) (<https://www.rfc-editor.org/rfc/rfc8617>)

Who's USING ARC IN PROD?

- Gmail
- Outlook
- Zoho
- Fastmail
- ProtonMail (New!)



<https://www.youtube.com/watch?v=V9kajr5dESs>

Chenkai Wang, Gang Wang // WWW'22 Talk: Revisiting Email
Forwarding Security under the Authenticated Received
Chain Protocol



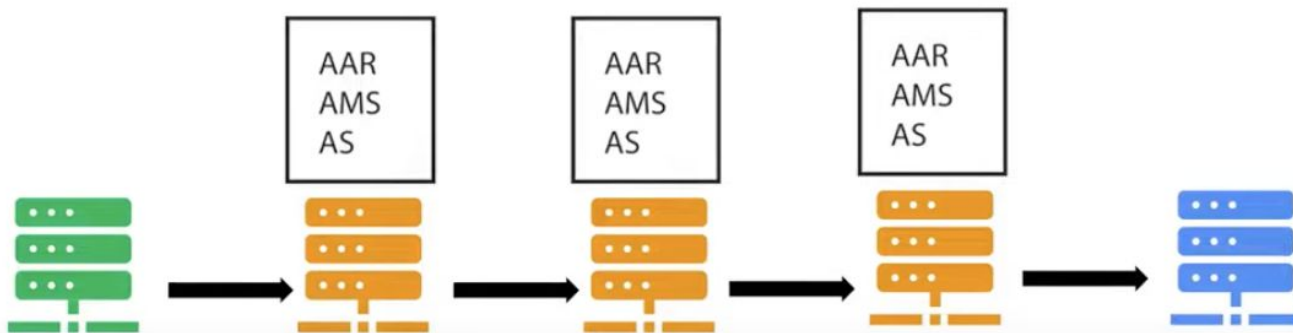
What's on the ARC Chain

Each forwarder adds the following headers to the message:

- **ARC-Authentication-Results** (AAR)
- **ARC-Message-Signature** (AMS)
- **ARC-Seal** (AS)

Altogether being one ARC Set.

$AAR_{(i)} = \{\text{SPF, DKIM, DMARC auth. result (i)th hop}\}$
 $AMS_{(i)} = \{\text{Signature of current msg body and headers}\}$
 $AS_{(i)} = \{\text{Signature of ARC chain, chain validity status}\}$



<https://www.youtube.com/watch?v=V9kair5dESs>

NORMAL AAR HEADER

What an AAR header is supposed to look like:

```
ARC-Authentication-Results: i=1; lists.example.org; spf=pass  
smtp.mfrom=jqd@d1.example; dkim=pass (512-bit key)  
header.i=@d1.example; dmarc=pass
```

<https://www.rfc-editor.org/rfc/rfc8617>

MAILCHANNELS AAR HEADER

This is what MCs AAR header ALWAYS looks like...

```
ARC-Authentication-Results: i=1; rspamd-9fcc56855-j2crh;  
auth=pass smtp.auth=cloudflare  
smtp.mailfrom=test@example.com
```

Wtf is auth=pass??

Where's my SPF/DKIM/DMARC checks??

<https://www.rfc-editor.org/rfc/rfc8617>



WHY CAN'T YOU JUST BE NORMAL?

MailChannels does not check SPF/DMARC/DKIM of the sender domain during the ARC chain

- Always claims “auth=pass” (?? what auth?)
 - Cloudflare account auth? CF Workers are publicly accessible...

<https://www.rfc-editor.org/rfc/rfc8617>

ARC's INFLUENCE ON SPAM SCORES

There's no way to know how the end receiver is making use of the AAR header results... However, we got hints:

ARC Authenticated Received Chain (ARC) permits intermediate email servers (such as mailing lists or forwarding services) to sign an email's original authentication results. This allows a receiving service to validate an email, in the event the email's SPF and DKIM records are rendered invalid by an intermediate server's processing. For more information, see [RFC 8617](#).

Enable the service, and enable ARC to override SPF, DKIM, and/or DMARC.

<https://docs.fortinet.com/document/fortimail/7.4.0/administration-guide/352990/configuring-antispam-profiles-and-antispam-action-profiles>

thanks Pancho ❤️

ARC'S INFLUENCE ON SPAM SCORES

The presence of an arc=pass generally guarantees a better spam score. Confirmed with ProtonMail. Seems to be the case with Gmail and Outlook as well.

- Red team pro tip!



ARC'S INFLUENCE ON SPAM SCORES

*You can also spoof emails from domains that don't have an SPF/DMARC record and it will likely land in the inbox!**

Around ~3114002316 (3 BILLION) domains don't have SPF/DMARC!**


**As long as the receiving email service adopted ARC*


****According to Project Sonar as of June 2023, this number includes subdomains**

MY BLACK HAT TALK GOT ACCEPTED???!

... even before I submitted it!

Blackhat CFP submission status

From  Blackhat CFP Review Board <cfp@blackhat.com>

☆  Feb 10, 2023

To byt3bl33d3r




Hello,

Congrats your talk got accepted!

DT

SPOOFING BLACKHAT.COM

- blackhat.com didn't have a SPF or DMARC record until sometime after Feb 2023
 - Notified DT & Grifter on Twitter Feb 2023
- ProtonMail takes ARC into consideration when determining an email's spam score.
- No SPF or DMARC contributes 0 to the Spam score
- ARC passing contributes -1! (lower the better)
- Goes straight to inbox 

HEADER TIME

02:45:51 10000

```
Authentication-Results: mailin039.protonmail.ch; dmarc=none (p=none dis=none)
  header.from=blackhat.com
Authentication-Results: mailin039.protonmail.ch; spf=none smtp.mailfrom=blackhat.com
Authentication-Results: mailin039.protonmail.ch; arc=pass smtp.remote-ip=23.83.212.17
  arc.chain=:mailchannels.net
Authentication-Results: mailin039.protonmail.ch; dkim=none
```

```
X-Spamd-Result: default: False [-1.10 / 25.00];
ARC_ALLOW(-1.00)[mailchannels.net:s=arc-2022:i=1]; MIME_GOOD(-0.10)[text/plain];
FROM_EQ_ENVFROM(0.00)[]; R_DKIM_NA(0.00)[]; RCVD_TLS_LAST(0.00)[]; ASN(0.00)[asn:36483,
ipnet:23.83.208.0/21, country:CA]; R_SPF_NA(0.00)[no SPF record];
NEURAL_HAM(-0.00)[-0.928]; DMARC_NA(0.00)[blackhat.com]; RCVD_COUNT_THREE(0.00)[4];
TO_MATCH_ENVRCPT_ALL(0.00)[]; MIME_TRACE(0.00)[0:+];
PREVIOUSLY_DELIVERED(0.00)[byt3bl33d3r@pm.me]; RCPT_COUNT_ONE(0.00)[1];
TO_DN_NONE(0.00)[]; FROM_HAS_DN(0.00)[]
```

X-Pm-Spamscore: 1

X-Pm-Spam-Action: inbox

DISCLAIMER++

Don't do crimes.

I'm not responsible if you do.

Only test on domains you own/control and have permission.

SPAMCHANNEL TESTER

<https://spamchannel.haxxx.workers.dev>

Code: <https://github.com/byt3bl33d3r/SpamChannel>

Based off of @ihsangan's CF worker code

Only test on domains you control!



DEMO: IMPERSONATING SATAN



“DISCLOSURE” TIMELINE

- Nov 2022 - Initial reachout by me via abuse@mailchannels.com (No official vulnerability reporting channel seemed to exist, was told about this email via social media)
 - MC response from Ken Simpson (CEO) saying that the SPF issue is known and not considered a vulnerability
 - Follow up by me saying if they'd reconsider because of how anyone can do this via CF workers
 - No further response
- Jan 2023 - Reachout by Rapid7
 - MC response from Ken Simpson (CEO) re-iterating they don't consider this an issue as they're primary customers are hosting companies who don't own the domains. Customers are welcome to secure their domain via DKIM + DMARC.
 - Rapid7 asks for confirmation that this issue won't be addressed by MC
 - No further response

“DISCLOSURE” TIMELINE

- *Jun 2023* - Sent final update summarizing findings and notifying them of Defcon talk
 - No response
- *Jul 2023* - MC sends me email saying they noticed I'm speaking about them at Defcon and if I'm willing to share details of my findings.
 - I remind them I've been in contact with their CEO since Nov 2022 and they already have all the details
 - CEO replies saying my emails were being sent to the wrong folder cause of a filter and didn't see them. Additionally, states they've introduced their “Domain Lockdown” feature on June 20th 2023 in order to solve this issue with CF workers.

TAKEAWAYS - IF YOU'RE A MAILCHANNELS CUSTOMER...

- As of June 20th 2023... Set your “Domain Lockdown” record ASAP!
 - A DNS TXT record specifically for MC
 - <https://support.mailchannels.com/hc/en-us/articles/16918954360845>

To lock the domain to a specific Cloudflare Workers account, use this syntax:

```
v=mc1 cfid=myapp.workers.dev
```

To block MailChannels from sending any emails from your domain, set the TXT record to show only the version string and no auth, senderid, or cfid fields, as follows:

```
v=mc1
```

TAKEAWAYS - IF YOU'RE A MAILCHANNELS CUSTOMER...

- CF workers will be required to set their “Domain Lockdown” record in order to send emails after a specific cutoff date (TBA). *You're still able to spoof all the things until then!*
- “Domain Lockdown” records will only be required for CF workers
 - from my understanding (?)
- Anyone is still able to sign up on MCs website and for 80\$ spoof all their customers via their SMTP relay. You're fully trusting in their mitigating controls.

TAKEAWAYS - IF YOU'RE AN ORG

- Identify if you're using MC (check your SPF for `"include:relay.mailchannels.net"`), put the "Domain Lockdown record" in ASAP.
- Make sure you have SPF/DMARC records on all domains even if you don't use them to send emails!
 - `"v=spf1 -all"`
- Display a banner on any email that doesn't have a DKIM signature but comes from a domain that's implemented DKIM (I've never seen this, I'm assuming possible?)

TAKEAWAYS - IF YOU'RE AN EMAIL SERVICE PROVIDER (E.G. GMAIL, OUTLOOK ETC..)

- Don't just bump the spam score of an email because arc=pass 🤖
- Actually check the AAR header?
- If you adopt ARC, you're at the mercy of the any instance in the chain that doesn't do their job...

TAKEAWAYS - IF YOU'RE AN EMAIL TRANSACTION SERVICE

- *Sender identity verification and/or Dedicated Sending IPs!*
 - Always do this...
- If you adopt ARC, do it well! Ask yourself “Do we need to even use ARC” in the first place...

TAKEAWAYS - EMAIL SECURITY

- ... still very brittle. Held up by duct tape and marinara sauce.
- Relies on orgs and users to do the right thing (good luck!)
- Very easy footguns
- ARC could incentivize a trend of “gaming the system” for better delivery rates if not implemented properly

SHOUT OUTS

- Chenkai Wang & Gang Wang
 - <https://gangw.web.illinois.edu/arc-www22.pdf>
 - <https://www.youtube.com/watch?v=V9kajr5dESs>
- @ihsangan
 - <https://gist.github.com/ihsangan/6111b59b9a7b022b5897d28d8454ad8d>
- Huge thanks to Rapid7, check out Project Sonar!
 - Curt Barnard
 - Matthew Kienow
 - Tod Beardsley
 - Spencer McIntyre
 - Caitlin Condon