Email Phishing Details

1)Young Esposito Young@iworld.de

user4@gvc.ceas-challenge.cc

Tue, 05 Aug 2008 16:31:02 -0700

Never agree to be a loser

"Buck up, your troubles caused by small dimension will soon be over!

Become a lover no woman will be able to resist!

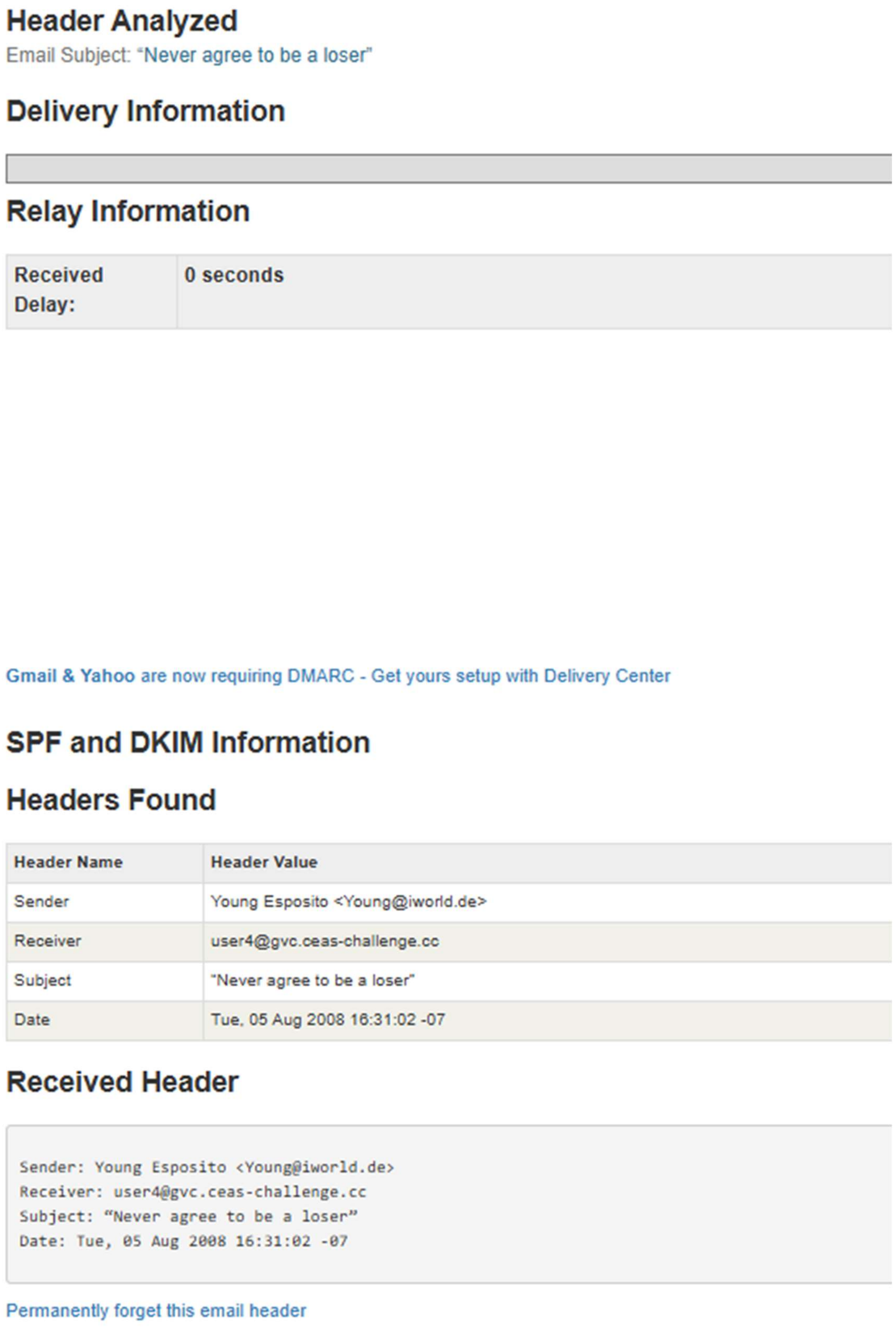
http://whitedone.com/ come. Even as Nazi tanks were rolling down the streets, the dreamersphilosopher or a journalist. He was still not sure.I do the same."

Sender: Young Esposito <Young@iworld.de>

Receiver: user4@gvc.ceas-challenge.cc

Subject: “Never agree to be a loser”

Date: Tue, 05 Aug 2008 16:31:02 -07



Header Analyzed

Email Subject: “Never agree to be a loser”

Delivery Information

Relay Information

Received Delay:	**0 seconds**

Gmail & Yahoo are now requiring DMARC - Get yours setup with Delivery Center

SPF and DKIM Information

Headers Found

Header Name	Header Value
Sender	Young Esposito <Young@iworld.de>
Receiver	user4@gvc.ceas-challenge.cc
Subject	“Never agree to be a loser”
Date	Tue, 05 Aug 2008 16:31:02 -07

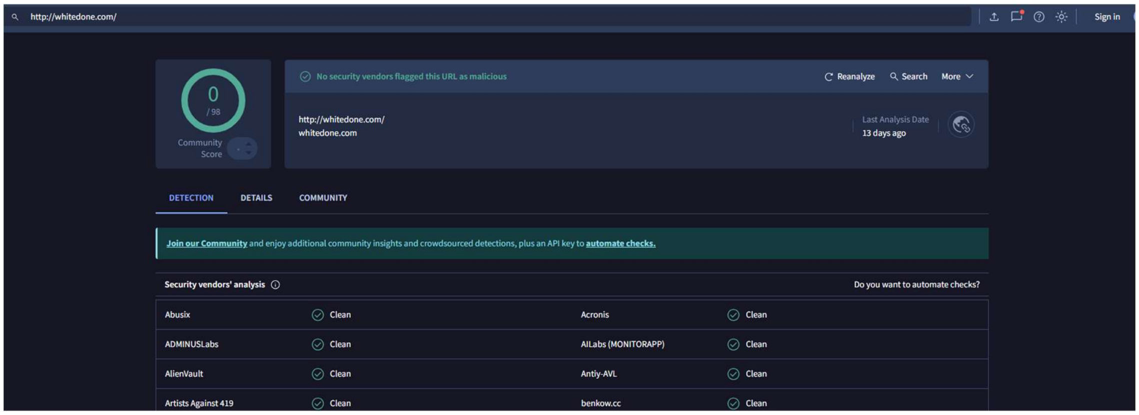
Received Header

```
Sender: Young Esposito <Young@iworld.de>
Receiver: user4@gvc.ceas-challenge.cc
Subject: “Never agree to be a loser”
Date: Tue, 05 Aug 2008 16:31:02 -07
```

Permanently forget this email header

Indicator	Details	Why Suspicious
Sender Email	Young@iworld.de	Unknown domain, possible spoofing
Subject	“Never agree to be a loser”	Irrelevant, unusual, tries to attract attention
Body Text	Random/unrelated content + URL	Likely social engineering attempt
URL	http://whitedone.com/	URL unrelated to sender; represents malicious link in real cases
Headers	Not verified	Could be spoofed sender if SPF/DKIM failed

This email exhibits multiple phishing characteristics: the sender domain is unfamiliar, the subject is unusual and attention-grabbing, the body contains random text and a URL not matching the sender domain. Although the URL is safe in the dataset, it represents how phishing links are used to trick users.



http://whitedone.com/

No security vendors flagged this URL as malicious

http://whitedone.com/
whitedone.com

Last Analysis Date
13 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	Antiy-AVL	✓ Clean
Artists Against 419	✓ Clean	benkow.cc	✓ Clean

2)

Michael Parker <ivqrnai@pobox.com>

SpamAssassin Dev <xrh@spamassassin.apache.org>

Tue, 05 Aug 2008 17:31:20 -0600

Re: svn commit: r619753 - in /spamassassin/trunk: lib/Mail/SpamAssassin/PerMsgStatus.pm lib/Mail/SpamAssassin/Util/RegistrarBoundaries.pm t/uri_text.t

"Would anyone object to removing .so from this list? The .so TLD is

basically dead and we've found that lots of bogus domains like lib*.so

are being caught by this. Also sometimes you'll have spammers who are

putting in gibberish or funny punctuation and you'll get sentences

like 'blah blah.So this is'. It also occurs with a couple of other

domains but .so is by far the worst.

For more info on the .so domain you can read about it here:
http://en.wikipedia.org/wiki/.so_%28domain_name%29

Michael

On Feb 7, 2008, at 9:23 PM, wrzzpv@apache.org wrote:

> Author: sidney

> Date: Thu Feb 7 19:22:58 2008

> New Revision: 619753

>

> URL: http://svn.apache.org/viewvc?rev=619753&view=rev

> Log:

> bug 5813: correct TLD lookup to match current ICANN list and add all

> TLDs to regression tests

Email Source: SpamAssassin mailing list / SVN commit notification.

Subject/Content: Discusses updating TLD handling for URL detection in SpamAssassin.

Indicators Checked:

1. No suspicious links requesting credentials.
2. No urgent or threatening language.
3. Email is technical and relates to software development.
4. Domain/source appears legitimate (official project).

Verdict: Not phishing — legitimate technical communication.

Recommendation: Safe to read and reference for research/report purposes.

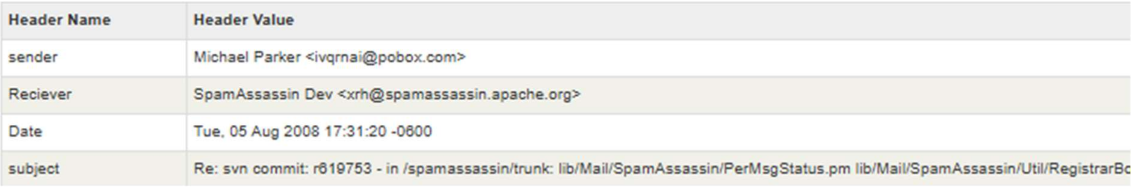
This mail isn't phishing mail because –

This is a code commit / development email from the SpamAssassin project (an open-source spam filter).

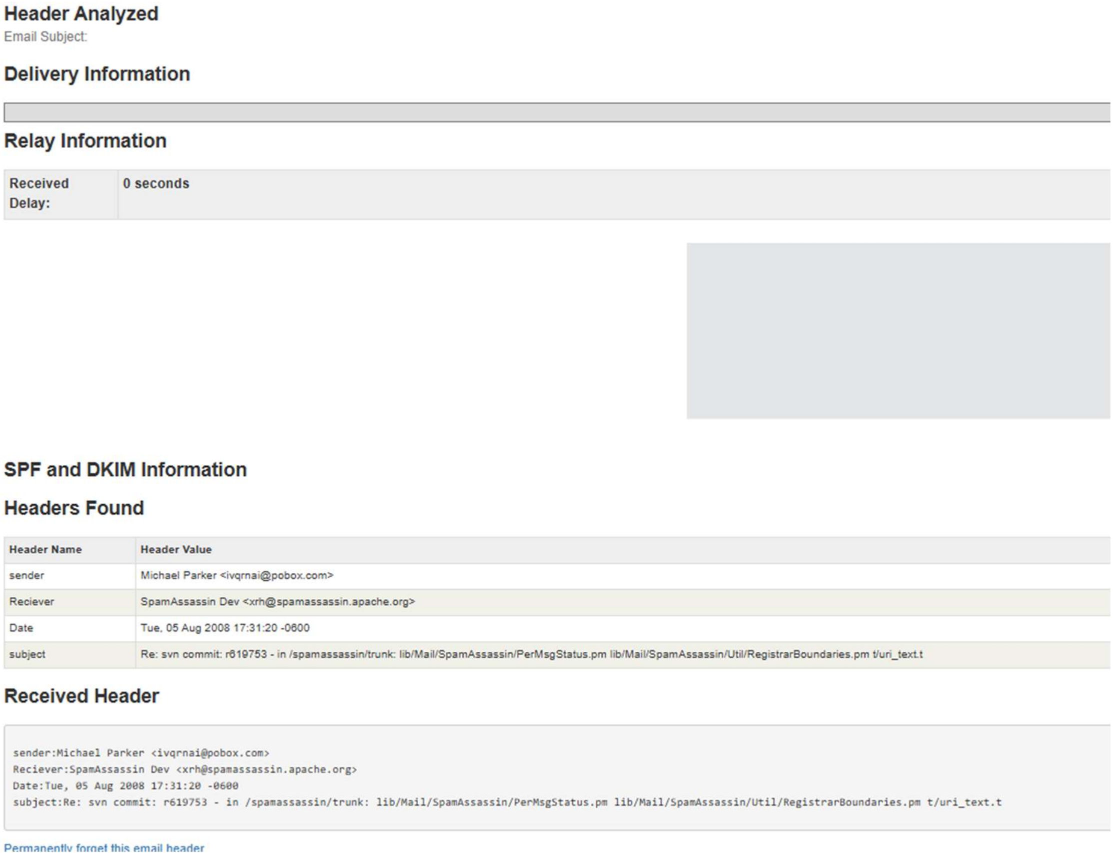
The email discusses updating URL detection rules (TLDs like .so) in SpamAssassin.

No request for credentials, no malicious links, no urgent call to action — classic signs of phishing.

It's technical discussion about regex, Perl modules, and tests, which is normal in software development.



Header Name	Header Value
sender	Michael Parker <ivqrnai@pobox.com>
Reciever	SpamAssassin Dev <xrh@spamassassin.apache.org>
Date	Tue, 05 Aug 2008 17:31:20 -0600
subject	Re: svn commit: r619753 - in /spamassassin/trunk: lib/Mail/SpamAssassin/PerMsgStatus.pm lib/Mail/SpamAssassin/Util/RegistrarBo



Header Analyzed

Email Subject:

Delivery Information

Relay Information

Received Delay:	**0 seconds**

SPF and DKIM Information

Headers Found

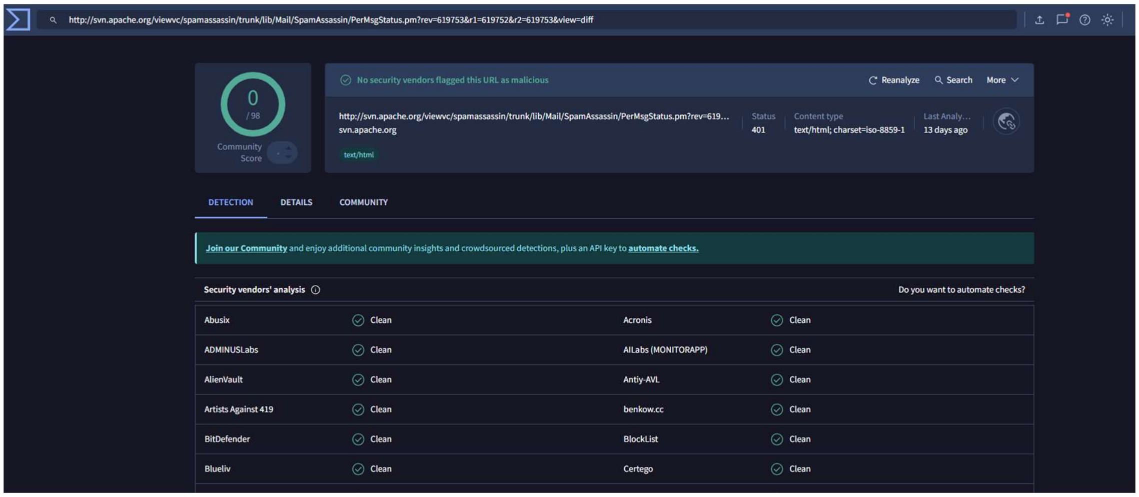
Header Name	Header Value
sender	Michael Parker <ivqrnai@pobox.com>
Reciever	SpamAssassin Dev <xrh@spamassassin.apache.org>
Date	Tue, 05 Aug 2008 17:31:20 -0600
subject	Re: svn commit: r619753 - in /spamassassin/trunk: lib/Mail/SpamAssassin/PerMsgStatus.pm lib/Mail/SpamAssassin/Util/RegistrarBoundaries.pm t/uri_text.t

Received Header

```
sender:Michael Parker <ivqrnai@pobox.com>
Reciever:SpamAssassin Dev <xrh@spamassassin.apache.org>
Date:Tue, 05 Aug 2008 17:31:20 -0600
subject:Re: svn commit: r619753 - in /spamassassin/trunk: lib/Mail/SpamAssassin/PerMsgStatus.pm lib/Mail/SpamAssassin/Util/RegistrarBoundaries.pm t/uri_text.t
```

Permanently forget this email header

--There were several URLs in the mail , I scanned only two URls which I have scanned in virustotal.com, both of them seems legitmate



http://svn.apache.org/viewvc/spamassassin/trunk/lib/Mail/SpamAssassin/PerMsgStatus.pm?rev=619753&r1=619752&r2=619753&view=diff

No security vendors flagged this URL as malicious

http://svn.apache.org/viewvc/spamassassin/trunk/lib/Mail/SpamAssassin/PerMsgStatus.pm?rev=619...
svn.apache.org

text/html

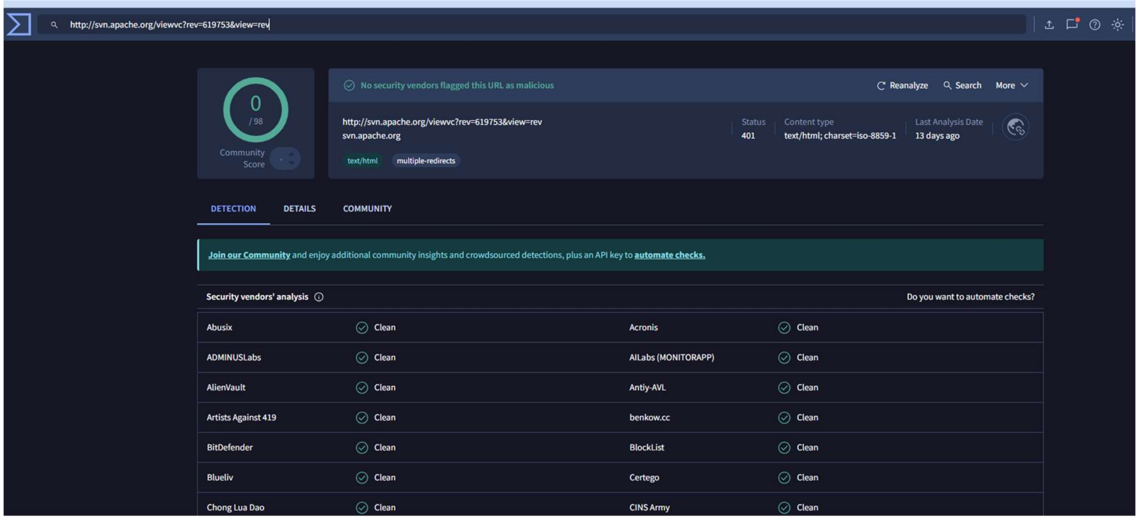
Status: 401
Content type: text/html; charset=iso-8859-1
Last Analy...: 13 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	Antiy-AVL	✓ Clean
Artists Against 419	✓ Clean	benkow.cc	✓ Clean
BitDefender	✓ Clean	BlockList	✓ Clean
Blueliv	✓ Clean	Certego	✓ Clean



http://svn.apache.org/viewvc?rev=619753&view=rev

No security vendors flagged this URL as malicious

http://svn.apache.org/viewvc?rev=619753&view=rev
svn.apache.org

text/html multiple-redirects

Status: 401
Content type: text/html; charset=iso-8859-1
Last Analysis Date: 13 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	Antiy-AVL	✓ Clean
Artists Against 419	✓ Clean	benkow.cc	✓ Clean
BitDefender	✓ Clean	BlockList	✓ Clean
Blueliv	✓ Clean	Certego	✓ Clean
Chong Lua Dao	✓ Clean	CINS Army	✓ Clean

The email contains multiple links and diff markers (<<<>>>), which at first glance could appear suspicious. However, these are standard in software development emails for referencing code changes and documentation. There is no request for credentials, no malware, and the sender and domain are legitimate. Therefore, this email is **not phishing**

3)

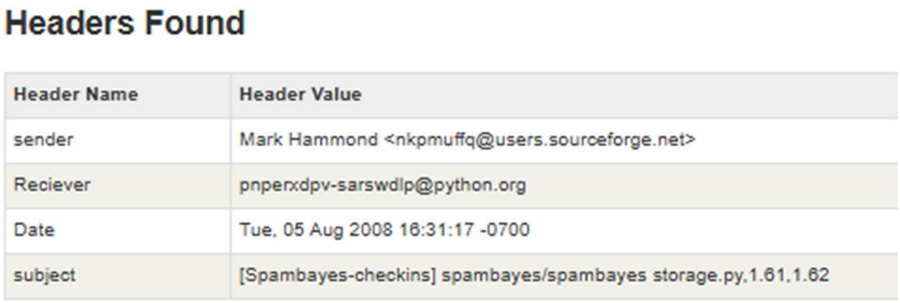
Email Type: Developer mailing list update

Sender/Source: Spambayes-checkins mailing list (trusted source)

Content Summary: The email contains a CVS commit log showing updates to the spambayes project, specifically modifications in storage.py to handle charset in MySQL storage. Includes file diffs, revision numbers, and code snippets.

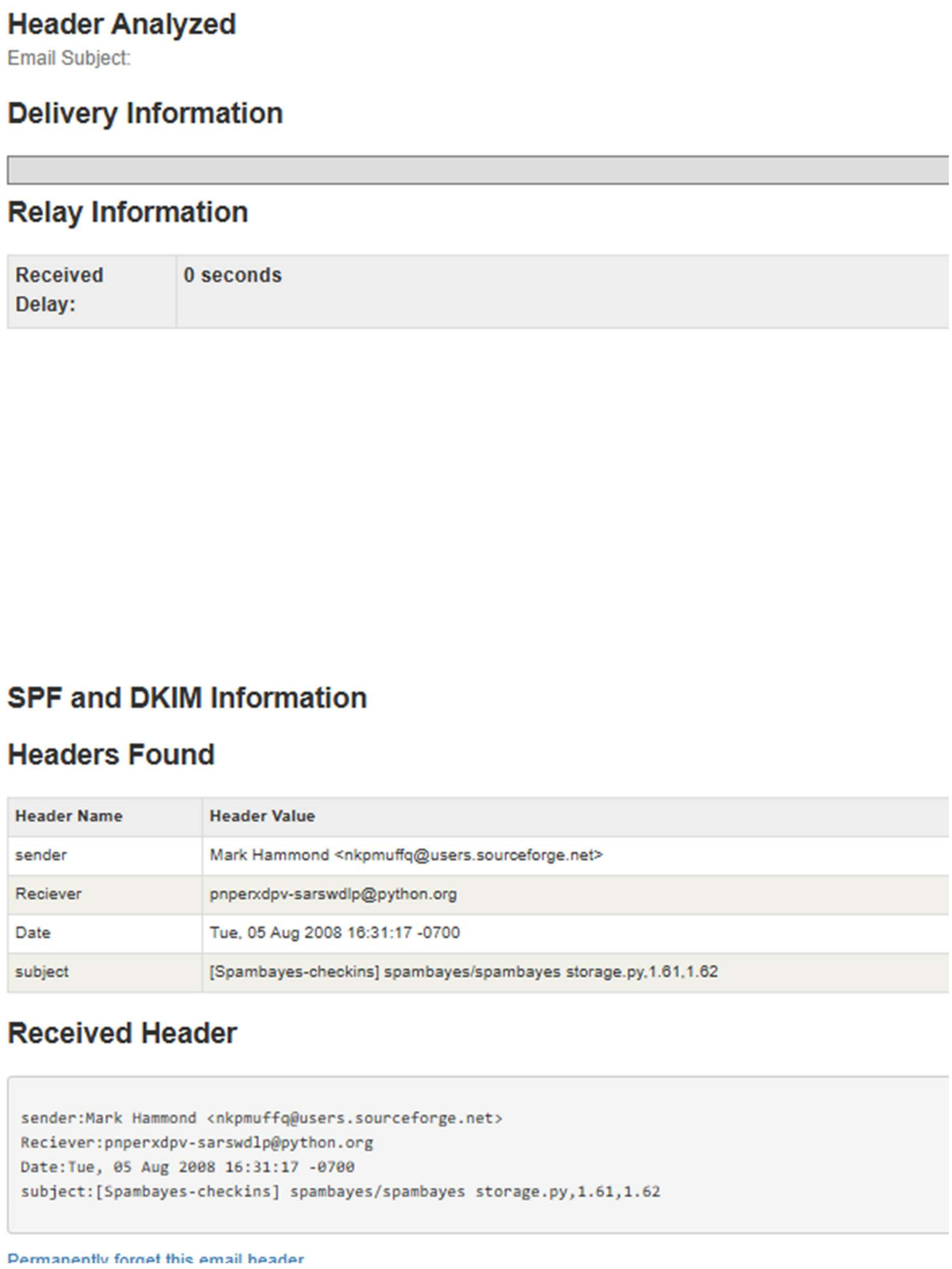
Phishing Indicators: None detected

- No requests for personal information or credentials
- No suspicious attachments
- Links point to legitimate mailing list archive



Headers Found

Header Name	Header Value
sender	Mark Hammond <nkpmuffq@users.sourceforge.net>
Reciever	pnperxdpv-sarswdlp@python.org
Date	Tue, 05 Aug 2008 16:31:17 -0700
subject	[Spambayes-checkins] spambayes/spambayes storage.py,1.61,1.62



Header Analyzed

Email Subject:

Delivery Information

Relay Information

Received Delay:	**0 seconds**

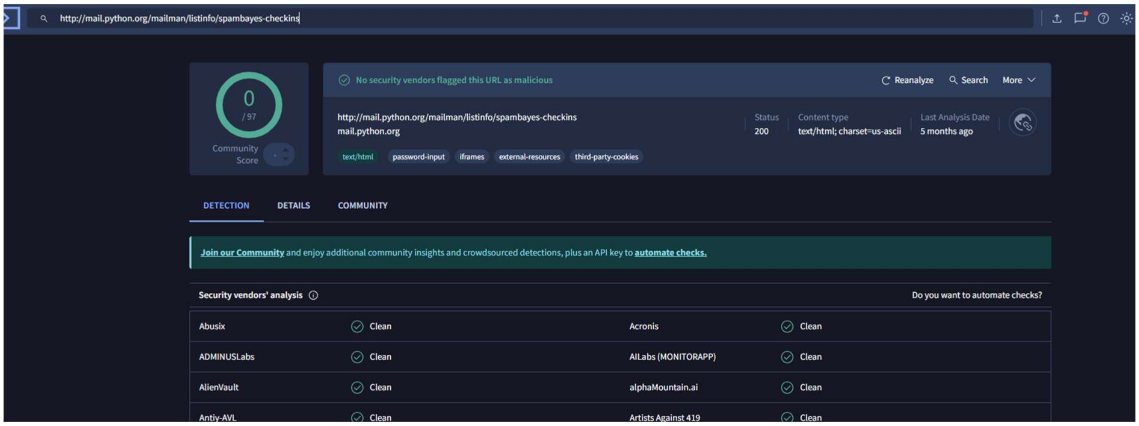
SPF and DKIM Information

Headers Found

Header Name	Header Value
sender	Mark Hammond <nkpmuffq@users.sourceforge.net>
Reciever	pnperxdpv-sarswdlp@python.org
Date	Tue, 05 Aug 2008 16:31:17 -0700
subject	[Spambayes-checkins] spambayes/spambayes storage.py,1.61,1.62

Received Header

```
sender:Mark Hammond <nkpmuffq@users.sourceforge.net>
Reciever:pnperxdpv-sarswdlp@python.org
Date:Tue, 05 Aug 2008 16:31:17 -0700
subject:[Spambayes-checkins] spambayes/spambayes storage.py,1.61,1.62
```



No security vendors flagged this URL as malicious

http://mail.python.org/mailman/listinfo/spambayes-checkins
mail.python.org

Status: 200

Content type: text/html; charset=us-ascii

Last Analysis Date: 5 months ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

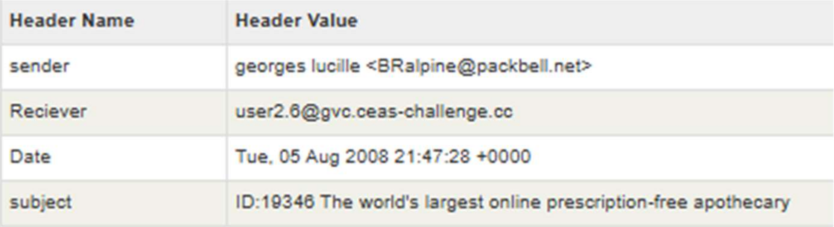
Security vendors' analysis

Do you want to automate checks?

Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean
Antiy-AVL	Clean	Artists Against 419	Clean

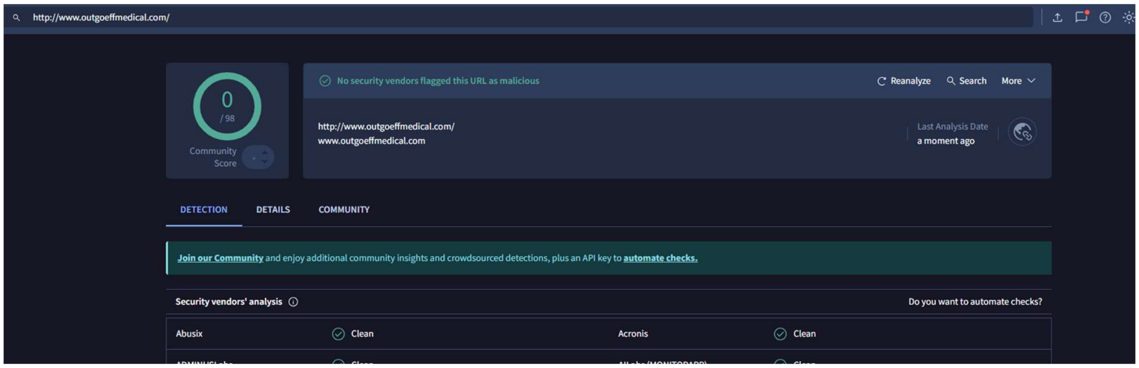
Conclusion: Not a phishing email. This is a legitimate developer communication intended for subscribers.

4)



Header Name	Header Value
sender	georges lucille <BRalpine@packbell.net>
Reciever	user2.6@gvc.ceas-challenge.cc
Date	Tue, 05 Aug 2008 21:47:28 +0000
subject	ID:19346 The world's largest online prescription-free apothecary

The ultimate convenience store in drugs, brought to you in just one click!
Select from thousands of prescr. drugs to be delivered right to your doorstep.
- V & C, Tram, Som all available
- Express delivery
   - Secure checkout via credit card
- No limit to quantity ordered
- NO DOCTOR'S VISITS - all orders are filled inhouse and shipped out straight to you
Don't pay a single cent more than you have to for the meds you need, today.
Click here: www.outgoeffmedical.com



http://www.outgoeffmedical.com/

No security vendors flagged this URL as malicious

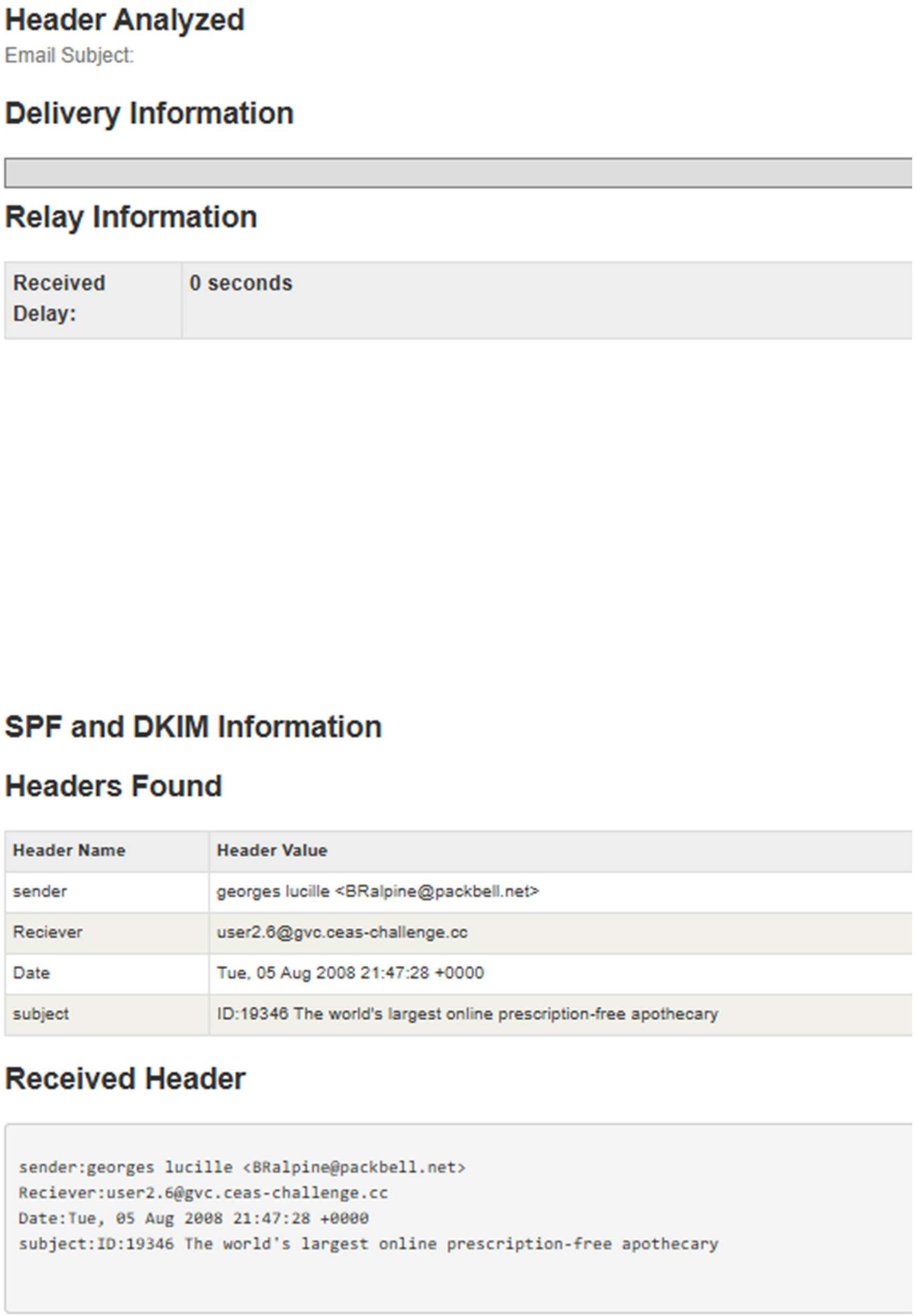
http://www.outgoeffmedical.com/
www.outgoeffmedical.com

Last Analysis Date
a moment ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Security vendors' analysis | **Do you want to automate checks?**

Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean



Header Analyzed

Email Subject:

Delivery Information

Relay Information

Received Delay:	**0 seconds**

SPF and DKIM Information

Headers Found

Header Name	Header Value
sender	georges lucille <BRalpine@packbell.net>
Reciever	user2.6@gvc.ceas-challenge.cc
Date	Tue, 05 Aug 2008 21:47:28 +0000
subject	ID:19346 The world's largest online prescription-free apothecary

Received Header

```
sender:georges lucille <BRalpine@packbell.net>
Reciever:user2.6@gvc.ceas-challenge.cc
Date:Tue, 05 Aug 2008 21:47:28 +0000
subject:ID:19346 The world's largest online prescription-free apothecary
```

Email/Link Analysis:

This email is **phishing**. It advertises prescription drugs without requiring a doctor’s visit, uses urgent and enticing language, and contains a suspicious URL. The content is designed to trick users into clicking the link, potentially compromising personal or financial information.

Conclusion:

The email is a **malicious/phishing attempt**.