What is That Email "Really" Telling Me
Understanding Email Header Spoofing

Keith Turpin
Chief Information Security Officer
Universal Weather and Aviation
March 2017
Introduction

Email is a business critical tool that isn't going away

It is also an open door to an organization's network and people

Criminals like open doors
Getting the Message

Email Spoofing: Altering email headers to make a message appear to come from somewhere other than the actual source

Fraudulent emails can impact an organization in two ways:
1. It can be the recipient of spoofed email
2. It can be the impersonated sender in email sent to other organizations

Impact:

1 billion dollars in e-mail business fraud losses reported over an 18-month period

1,300% increase
Objectives

This presentation is intended to help IT and security teams:

- Better understand the mind of the attacker
- Identify meaningful email header information
- Determine an email's lifecycle
- Quickly identify spoofed email
- Help business partners understand when you are the spoofed sender
- Identify services and accounts used for reporting abuse and compromises
- Build a story around a spoofing event, which can be used for end user education
- Understand some defensive strategies
# Email Attack Roundup

1. Marketing and other generic spam
2. Email address validation
3. Dragnet phishing
4. Spear Phishing
5. Fake news or social engineering
6. Malicious payloads
7. Links to malicious payload websites
8. Attachments with embedded links to malicious payload sites
9. Links to impersonated login sites
Message vs Envelope Headers

Message headers are used by people

Envelope headers are used by the SMTP server

Message Headers are visible in the email

Envelope Headers contain routing details

The email Message Headers are contained in the Envelope Header

Note: this example shows content from two different email
Viewing Headers

Headers in Outlook

Headers in Gmail
Envelope Header Breakdown

Envelope Headers contain many fields, but these are most important

**Return-Path:**
- Delivery issue notices are sent to this address
- Validated by SPF

**Reply-To:**
- Email address used in message replies
- Overrides the "From" address in replies

**Received:**
- A single email will often have several "Received" entries
- The bottom "Received" entry will show the first server to handle the message

**Lines beginning with X-:**
- Extra data that is not contained in any standard
- Added by email servers and security tools

**NOTE:** Received and X- fields created by your own email services are the only completely trustworthy entries
Example 1: Header Walk Through

From: CFO [mailto:CFO@universalweather.com]  
Sent: Monday, January 23, 2017 11:51 AM  
To: melody.*****@universalweather.com  
Subject: Melody  

Hi Melody,  

I want you to send me the list of W-2 copy of employees wages and tax statement for 2016, I need them in PDF file type. Kindly prepare the lists and email them to me asap.  

Regards,  
CFO

--- Internal routing above top line removed for example ---

Received: from p3plwbeout24-04.prod.phx3.secureserver.net ([68.178.252.188] verified) by *******.univ-wea.com (#.##.#.59/#.##.#.59) with ESMTPS id v0QD1jq4014164 for melody.*****@universalweather.com; Mon, 23 Jan 2017 11:51:12 -0600  
Received: from localhost ([68.178.252.152]) by p3plwbeout24-04.prod.phx3.secureserver.net with bizsmtp id btrB1u0013J2rYL01trBCG; Mon, 23 Jan 2017 10:51:11 -0700  
Received: (qmail 16608 invoked by uid 99); 23 Jan 2017 17:51:11 -0000  
Content-Type: text/html; charset="utf-8"  
User-Agent: Workspace Webmail 6.6.1  
X-Originating-IP: 154.118.68.169  
Message-ID: <20170123105110.813345af76f4fb74a86b6ef72a8b63d9.1d3ff0a611.wbe@email24.godaddy.com>  
From: CFO <CFO@universalweather.com>  
X-Sender: andy.farrell@henleyfineart.com  
Reply-To: CFO <CFO@highmail.net>  
To: <melody.*****@universalweather.com>  
Subject: Melody  
Date: Mon, 23 Jan 2017 10:51:10 -0700  
MIME-Version: 1.0  
Return-Path: andy.farrell@henleyfineart.com

GoDaddy email service

GoDaddy IP

GoDaddy IP

Internal handoff

GoDaddy Webmail Service

GoDaddy uses the X-Originating-IP header which is the IP of the client accessing the service

Reply-To Domain does not match "From" domain. This is where attacker is waiting for response

Does not match "From" address
Example 1: Where is Highmail.net

We know the email was forged, but we can learn a lot looking into:

- **Reply-To:** CFO@highmail.net
- **X-Originating-IP:** 154.118.68.169
- **Return-Path:** andy.farrell@henleyfineart.com
Example 1: Who is highmail.net

Spammer and email fraudsters often setup throw away domains

- **Reply-To:** CFO CFO@highmail.net
- **X-Originating-IP:** 154.118.68.169
- **Return-Path:** andy.farrell@henleyfineart.com

---

**Whois Lookup related to highmail.net**

<table>
<thead>
<tr>
<th>Domain Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain: highmail.net</td>
</tr>
<tr>
<td>Registrar: NAMESilo, LLC</td>
</tr>
<tr>
<td>Registration Date: 2016-12-26</td>
</tr>
<tr>
<td>Expiration Date: 2017-12-26</td>
</tr>
<tr>
<td>Updated Date: 2016-12-26</td>
</tr>
<tr>
<td>Status: clientDeleteProhibited</td>
</tr>
<tr>
<td>clientRenewProhibited</td>
</tr>
<tr>
<td>clientTransferProhibited</td>
</tr>
<tr>
<td>clientUpdateProhibited</td>
</tr>
<tr>
<td>Name Servers: ns1.ghoster.net</td>
</tr>
</tbody>
</table>

**Registrant Contact**

- **Name:** Domain Administrator
- **Organization:** See PrivacyGuardian.org
- **Street:** 1928 E. Highland Ave. Ste F104 PMB# 255
- **City:** Phoenix
- **State:** AZ
- **Postal Code:** 85016
- **Country:** US
- **Phone:** 1.3478717726
- **Email:** email@privacyguardian.org

---

The highmail.net domain was just created in Dec 2016

Actual Registrar hidden through use of PrivacyGuardian

Privacy Guardian has an abuse reporting form, but my report went unanswered
Example 1: Who is highmail.net

If the information is valid, the culprit was far away

- Reply-To: CFO CFO@highmail.net
- X-Originating-IP: 154.118.68.169
- Return-Path: andy.farrell@henleyfineart.com

Client location based on IP registration.
Example 1: Looking into henleyfineart.com

Contacting providers and other parties associated with a fraud email may break the attack chain and provide notification to other victims

- **Reply-To:** CFO CFO@highmail.net
- **X-Originating-IP:** 154.118.68.169
- **Return-Path:** andy.farrell@henleyfineart.com

**Checking henleyfineart.com when incident first occurred**

![Welcome to henleyfineart.com](https://www.godaddy.com)

This Web page is parked FREE, courtesy of GoDaddy.

**Follow-up after reporting issue to GoDaddy**

![Not Found](https://www.godaddy.com)

HTTP Error 404. The requested resource is not found.

**Regarding henleyfineart.com**

1. Email fraudsters will often alter the Return-Path to show a different domain located on the same hosting provider. This gives them the same IP range for source verification, while pointing the finger at someone else.

2. henleyfineart.com could have been legitimately compromised and been the true source of the email.
Mounting a Defense

Email Fraud is a like a three legged stool that relies on multiple exploit paths to succeed:

1. People ....................... *Trained, tested and informed*
2. Business Process ...... *Out of band verifications and incident reporting*
3. Technology ............... *Email security gateways*
   - Web security gateway
   - SPF, DKIM and DMARC
   - Suspicious email tagging

Break any one leg, and the whole scam comes tumbling down
Important: Envelope Headers are lost when messages are forwarded!

Always have users create a new email, then attach the suspicious email to the new message. Sending the original message as an attachment, preserves the headers.
Technology - SPF, DKIM and DMARC

(SPFW) Sender Policy Framework:
Looks up the domain in the "Return-Path" (the SMTP envelop sender) and verifies that the corresponding IP is authorized to send email for that domain

- Does not prevent attackers from spoofing the "From" address

(DKIM) DomainKeys Identified Mail:
Digitally signs emails and the receiver runs a DNS query to get the public key from the sender domain

- Does not prevent attackers from spoofing the "From" address
- Can validate message integrity

(DMARC) Domain-based Message Authentication, Reporting and Conformance:
Builds upon both the DKIM and SPF specifications

- Verifies the "From" domain matches the "Return-Path" domain checked by SPF
- Verifies the "From" domain matches the “d= domain name” in the DKIM signature
Questions
Example 2: London Traffic Ticket

NOTE: Actual London Borough of Barking and Dagenham website: www.lbbd.gov.uk

Redirects to:

thebridgewatertriangledocumentary.com/wp-content/plugins/woocommerce/np613ysi/pdgdk0ft.php

hw4t.cpsnorthernonline.com/local/CPS_Enforcement/options/parking_ticket.php

Social media links go to authentic Borough sites
Example 2: More Domains in the Header

Received: from kvm42.bva-persona.com (kvm42.bva-persona.com [185.117.74.234])
    by xxxxxxxx.univ-wea.com (#.##.0.59/#.##.0.59) with ESMTPS id
    v0QD1jq4014164 for <sean.*******@univ-wea.com>; Thu, 26 Jan 2017 07:01:53 -0600
Message-ID: <A8521AE41BCFE3F02C2960DFDB0E56DB@lbbdwork.com>
Return-Path: support@lbbdwork.com
From: London Borough of Barking and Dagenham Council <support@lbbdwork.com>
To: <sean.******@univ-wea.com>
Subject: Email ID RSU – Announcement for (PCN) Owner
Date: Thu, 26 Jan 2017 14:01:50 +0100
Organization: London Borough of Barking and Dagenham Council

Sending email server
Different domain set for Return-Path
### Example 2: Disposable Domains for Scam

#### Addresses of Interest:

<table>
<thead>
<tr>
<th>Email Server:</th>
<th>cpsnorthernonline.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Return-Path:</td>
<td>lbbdwork.com</td>
</tr>
<tr>
<td>Link Path:</td>
<td>thebridgewatertriangledocumentary.com</td>
</tr>
<tr>
<td>Redirect:</td>
<td>bva-persona.com [185.117.74.234]</td>
</tr>
</tbody>
</table>

#### Domain Information:

**lbbdwork.com**

- **Domain**: lbbdwork.com
- **Registrar**: NAMESILO, LLC
- **Registration Date**: 2017-01-25
- **Expiration Date**: 2018-01-25
- **Updated Date**: 2017-01-25

**cpsnorthernonline.com**

- **Domain**: cpsnorthernonline.com
- **Registrar**: NAMESILO, LLC
- **Registration Date**: 2017-01-29
- **Expiration Date**: 2018-01-29
- **Updated Date**: 2017-01-29

#### Registrant Contact:

- **lbbdwork.com**
  - **Name**: Domain Administrator
  - **Organization**: See PrivacyGuardian.org

- **cpsnorthernonline.com**
  - **Name**: Domain Administrator
  - **Organization**: See PrivacyGuardian.org

- **Registered at time of scam**

- **Actual registrar hidden**: This looks familiar
### Example 2: London Traffic Ticket

#### Addresses of Interest:

<table>
<thead>
<tr>
<th>Address Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Server</td>
<td>cpsnorthernonline.com</td>
</tr>
<tr>
<td>Return-Path</td>
<td>lbbdwork.com</td>
</tr>
<tr>
<td>Link Path</td>
<td>thebridgewatertriangledocumentary.com</td>
</tr>
<tr>
<td>Redirect</td>
<td>bva-persona.com [185.117.74.234]</td>
</tr>
</tbody>
</table>

Although relatively new, this appears to be a legitimate registration. Webserver may have been compromised, but it is off line now.

The appears to be a legitimate domain and site and webserver may have been compromised for redirect.
Example 2: The Borough's Were Notified

After being notified the Boroughs quickly posted notifications to their website and social media.

Fake Council Parking Ticket notice

Please be aware that if you have received an email that looks like an official Council parking penalty it is a FAKE.

The Council would never issue a parking fine by email.

Please do NOT click on any link or call or email the Council but delete the email instead.

Warning over fake parking ticket issued

Please keep an eye out for a fake email which fraudulently claims to be from Barking and Dagenham Council claiming you have been issued with a parking ticket.

If you receive an email, do not click the links. Head to our website and search for PCN, you can then enter the PCN number to check if it is legitimate.

We are currently investigating this matter.
Useful Resources

Checking Risky Attachments
- iGuardian on the InfraGard Portal has a file upload and malware check
- Virus Total (file and website scanning): https://www.virustotal.com
- Malwr: https://malwr.com/
- Sucuri SiteCheck (website checker): https://sucuri.net/scanner/

Email Blacklist Checking Sites:
- Barracuda Reputation Block List (BRBL): http://barracudacentral.org/rbl
- SORBS SPAM Blacklist: http://www.sorbs.net/lookup.shtml
- Spamhaus blocklist: https://www.spamhaus.org/

Open email Relay testing tools:
- Mail Radar: http://www.mailradar.com/openrelay/
- DNS Goodies (lots of site analysis tools): http://dnsgoodies.com/
- Spam Help Open Relay test: http://www.spamhelp.org/shopenrelay/

Anti-Phishing Working Group (APWG)
An international coalition seeking to unify the global response to cybercrime across industry, government and law-enforcement sectors. APWG’s membership includes more than 1800 Institutions worldwide: http://www.antiphishing.org/

Best resource for Information on SPF, DKIM and DMARC:
https://blog.returnpath.com/how-to-explain-spf-in-plain-english
https://blog.returnpath.com/how-to-explain-dmarc-in-plain-english