Lab - Email Header Analysis

Overview

In this lesson, you will learn the fundamentals of analyzing the contents of an email header. Analyzing email headers is one of the most common tasks in digital forensics and can help authenticate an email sender. An example of practical use of a mail header analysis would be establishing the true identity of the email sender or receiver in a court of law. By analyzing the contexts of an email header, digital forensic experts can examine the authentication keys to determine if an email sender was forged.

Terms used in this lab

Sender Policy Framework (SPF)

SPF is a framework to prevent sender address forgery. In addition, the SPF field describes mail servers that are allowed to send messages for the given (sender) domain. SPF thus helps to avoid fake sender email addresses. The result (Received-SPF) can be neutral, pass or fail but, this is not always the case. The SPF should not be used to confirm the legitimacy of the email. The following example came from a fake email.

Example:

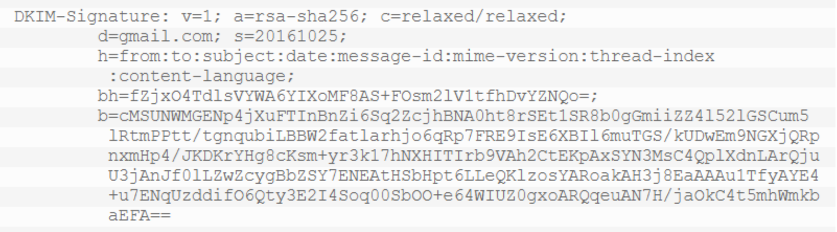
```
Received: from sv323.xserver.jp (sv323.xserver.jp. [219.94.203.163])
        by mx.google.com with ESMTPS id
j17si21147467pll.154.2021.06.01.07.09.37
        (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
        Tue, 01 Jun 2021 07:09:38 -0700 (PDT)
Received-SPF: neutral (google.com: 219.94.203.163 is neither permitted nor
denied by best guess record for domain of n-satou@saho.co.jp) client-
ip=219.94.203.163;
```

Domain Keys Identified Mail (DKIM)

DKIM is a method used to associate a domain name to an email. DKIM allows an organization to check the (cryptographic) signature to ensure untampered transit of the message and true ownership of the message.

Not every email is going to have this feature.

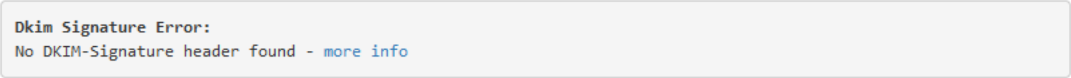
Example



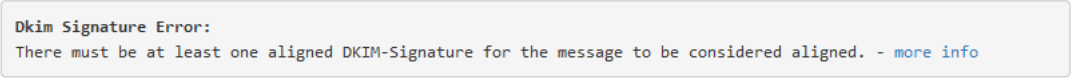
```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20161025;
        h=from:to:subject:date:message-id:mime-version:thread-index
         :content-language;
        bh=fZjxO4TdlsVYWA6YIXoMF8AS+FOsm2lV1tfhDvYZNQo=;
        b=cMSUNWMGENp4jXuFTInBnZi6Sq2ZcjhBNA0ht8rSEt1SR8b0gGmiiZZ4l52lGSCum5
         lRtmPPtt/tgnqubiLBBW2fatlarhjo6qRp7FRE9IsE6XBIl6muTGS/kUDwEm9NGXjQRp
         nxmHp4/JKDKrYHg8cKsm+yr3k17hNXHITIrb9VAh2CtEKpAxSYN3MsC4QplXdnLArQju
         U3jAnJf0lLZwZcygBbZSY7ENEAtHSbHpt6LLeQKlzosYARoakAH3j8EaAAAu1TfyAYE4
         +u7ENqUzddifO6Qty3E2I4Soq00SbOO+e64WIUZ0gxoARQqeuAN7H/jaOkC4t5mhWmkb
         aEFA==
```

If the DMIK is legit and can be confirmed as originating from a real domain, you will see the following message: `dkim=pass`

During the analysis of any email header, if the DKIM is missing, you may see something similar to the following message.



```
Dkim Signature Error:
No DKIM-Signature header found - more info
```



```
Dkim Signature Error:
There must be at least one aligned DKIM-Signature for the message to be considered aligned. - more info
```

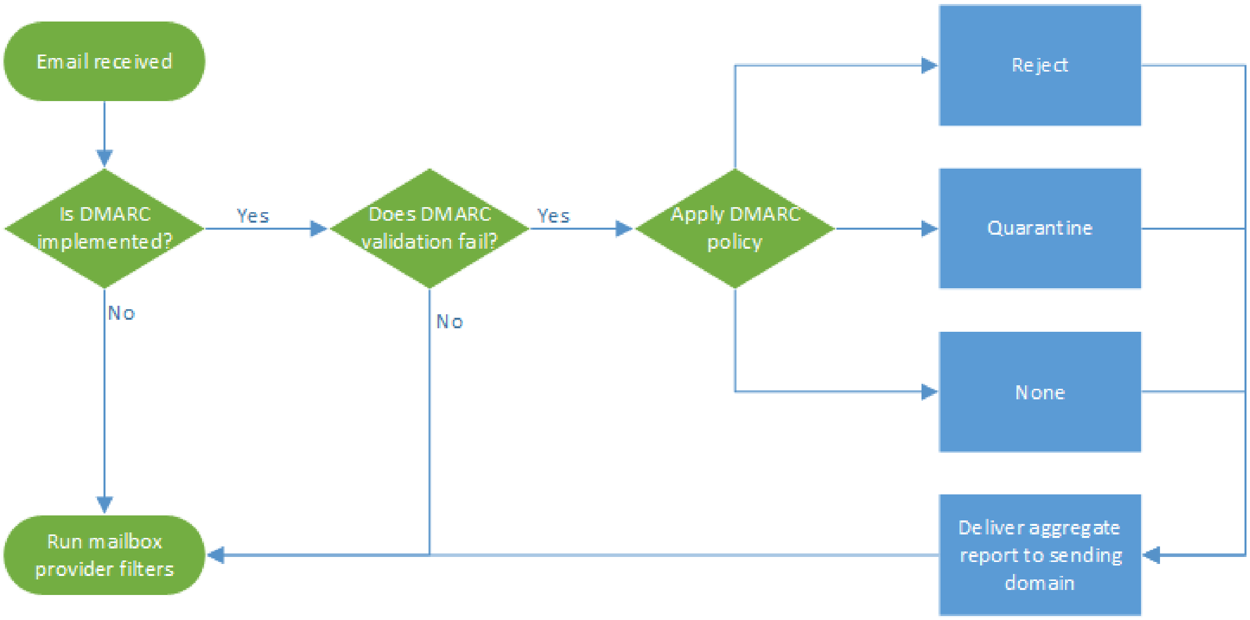
The fact that the DKIM is missing only indicates that the sender was not using the protocol, and not all senders legit or otherwise will use DKIM but, no DKIM and no SPF means, no DMARC.

Domain Based Message Authentication Reporting (DMARC)

The **Domain Based Message Authentication Reporting** (DMARC) security email protocol leverages DNS and uses the **Sender Policy Framework (SPF)** and **DomainKeys Identified Mail (DKIM)** open protocols to verify email senders.

The DMARC record check and detects any misalignment between an email sender and the address as it appears in the FROM field as seen by the email recipient. In that case, DMARC activates an administered protocol that tells the receiving server to either accept the message, quarantine the message, or reject it as defined in the sender's usage policy.

As part of the validation process, the DMARC provides the sender reports on who is attempting to use their domain to send messages. This visibility allows the sender to fine-tune their policy as new threats emerge. In this way, DMARC helps companies establish brand trust by reducing nonvalidated or fraudulent email threats.


Email received
Is DMARC implemented?
Yes
No
Does DMARC validation fail?
Yes
No
Apply DMARC policy
Reject
Quarantine
None
Deliver aggregate report to sending domain
Run mailbox provider filters

Start the lab!

In this example, I have chosen an incoming email marked as SPAM for analysis.

Hello Sir!

Greetings And How Are You Today? With Regards …..My name is Dennis Olisa a bank manager here in Zenith Bank I contacted you because I have something good I want us to partner and work together that will benefit the both of us. To explain more details to your better understanding, I will advise you to reply back to enable me to introduce myself to you and the reason why I am contacting you in this matter.

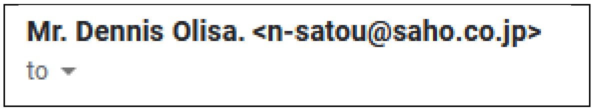
Thank you. I wish you a wonderful weekend, take proper care of yourself.

Best regards,

Mr. Dennis Olisa.

Examine the sender's email address

Starting with the sender's email, we see that the message is probably bogus. Not even an attempt to spoof the address to indicate it came from Zenith bank. This email appears to have originated from a mail server located in Japan.

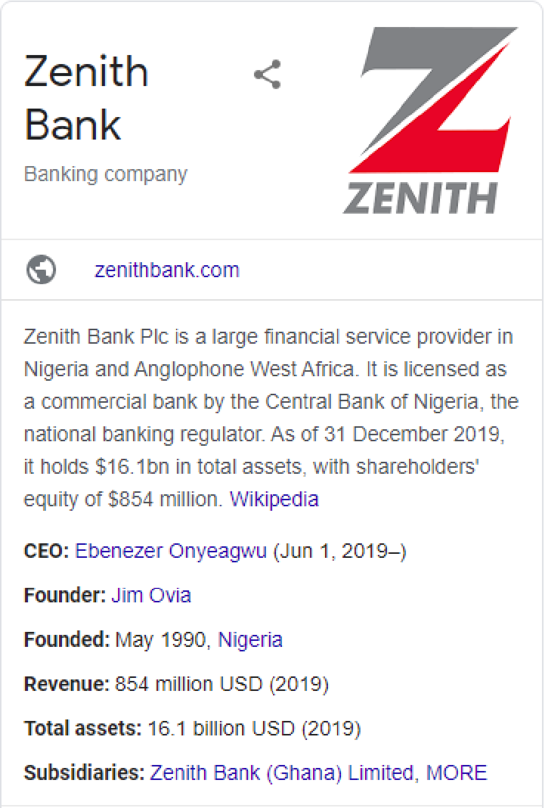


Mr. Dennis Olisa. <n-satou@saho.co.jp>
to

Using Google to verify information in the email

We next do a Google search to gather information about the **Zenith Bank** and if **Dennis Olisa** is an actual person.

First, let us look at what we know about the Zenith Bank. The bank is legit, but **Dennis Olisa** is not the bank manager; he is listed as the executive director.



Zenith Bank

Banking company

zenithbank.com

Zenith Bank Plc is a large financial service provider in Nigeria and Anglophone West Africa. It is licensed as a commercial bank by the Central Bank of Nigeria, the national banking regulator. As of 31 December 2019, it holds $16.1bn in total assets, with shareholders' equity of $854 million. Wikipedia

CEO: Ebenezer Onyeagwu (Jun 1, 2019–)

Founder: Jim Ovia

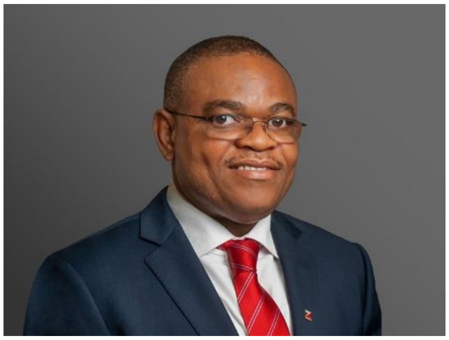
Founded: May 1990, Nigeria

Revenue: 854 million USD (2019)

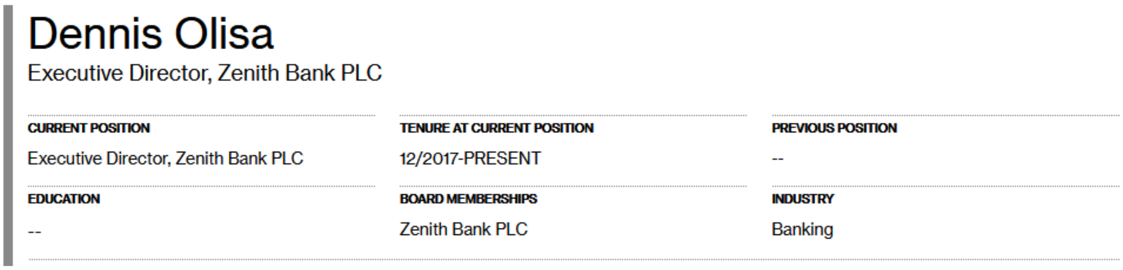
Total assets: 16.1 billion USD (2019)

Subsidiaries: Zenith Bank (Ghana) Limited, MORE

Under Google images, we find his photo.



Using Google search, we find some bio information.



Dennis Olisa

Executive Director, Zenith Bank PLC

CURRENT POSITION	TENURE AT CURRENT POSITION	PREVIOUS POSITION
Executive Director, Zenith Bank PLC	12/2017-PRESENT	--
EDUCATION	**BOARD MEMBERSHIPS**	**INDUSTRY**
--	Zenith Bank PLC	Banking

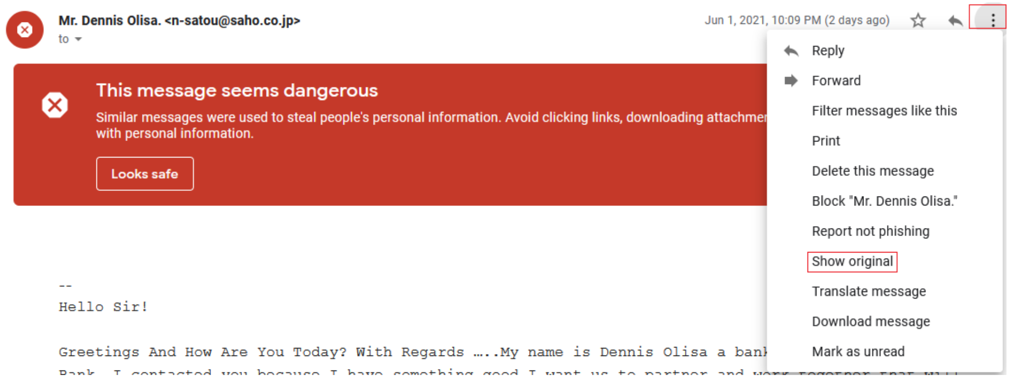
Email Header Analysis

Moving on with our analysis, we next examine the header information to find out where this email originated from and who sent it. If we are lucky, we might even be able to Google earth the originating IP address of the sender and see the actual location from where the email was sent from.

Viewing email headers

The easiest way to view the header information of an email sent to a Gmail or Yahoo account is to use the built-in tools both providers provide.

To view the header information of an email inside of Gmail’s webmail, open the email and expand the options on the right of the viewing pane. From the context menu, select show original.



Mr. Dennis Olisa. <n-satou@saho.co.jp>
to

Jun 1, 2021, 10:09 PM (2 days ago)

This message seems dangerous

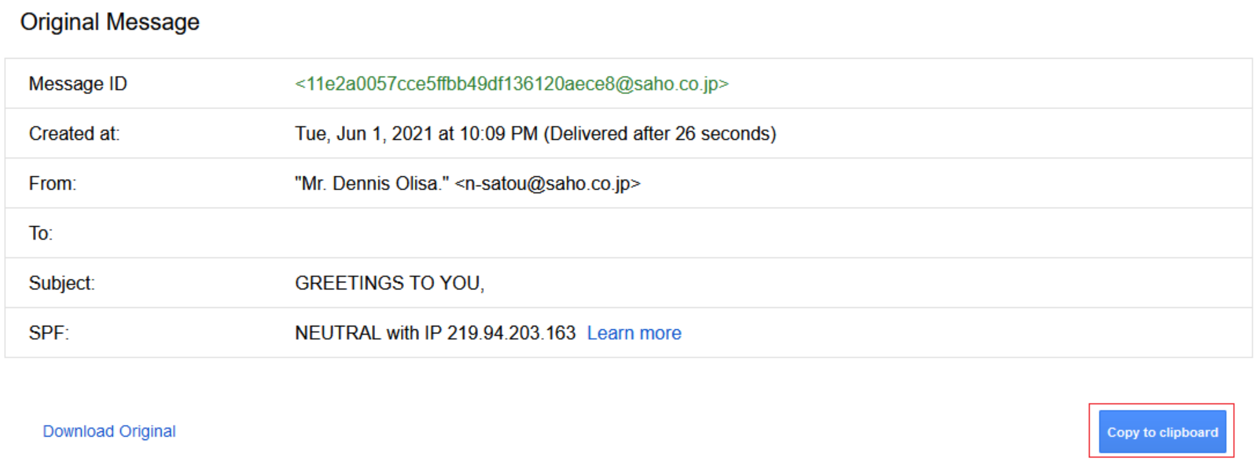
Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachme with personal information.

Looks safe

```
--
Hello Sir!

Greetings And How Are You Today? With Regards ....My name is Dennis Olisa a bank
Bank. I contacted you because I have something good I want us to partner and work together that will
```

We are shown the header information. The information is revealed to us is in two parts. The first is a summary of the email.



Original Message

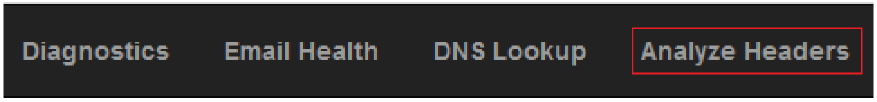
Message ID	<11e2a0057cce5ffbb49df136120aece8@saho.co.jp>
Created at:	Tue, Jun 1, 2021 at 10:09 PM (Delivered after 26 seconds)
From:	"Mr. Dennis Olisa." <n-satou@saho.co.jp>
To:	
Subject:	GREETINGS TO YOU,
SPF:	NEUTRAL with IP 219.94.203.163 Learn more

The second or bottom part shows the header information. To help us better analyze the header information were going to use an online tool provided by MXToolbox. In the bottom right corner of your email header summary, click on the blue box marked, **Copy to clipboard**.

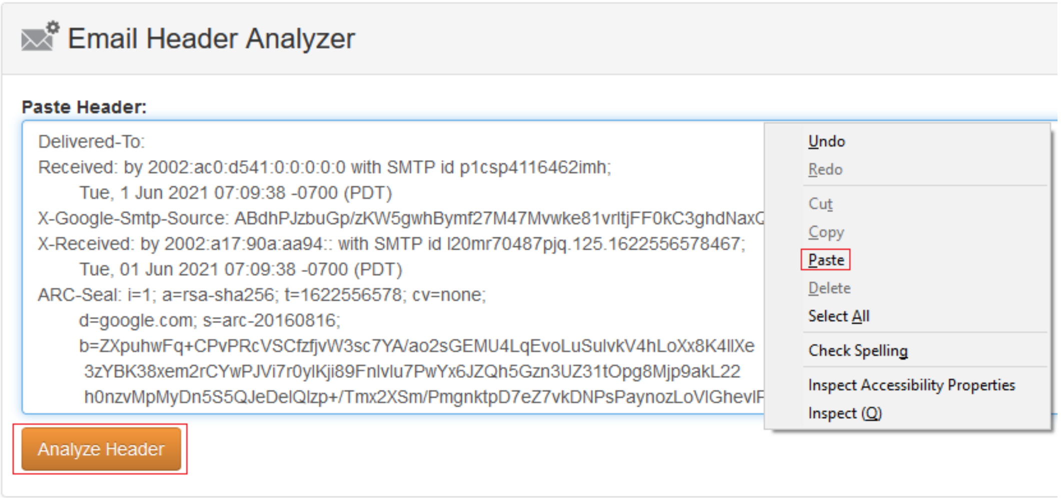
Open a browser, and in the address bar, type `mxtoolbox.com`.

https://mxtoolbox.com

From the taskbar, click the link for **Analyze Headers.**



In the text box, right-click, and from your context menu, select paste (Ctrl+v). Once you have the header information pasted in the text box, click on the orange button labeled Analyze Header in the lower left-hand corn**er.**



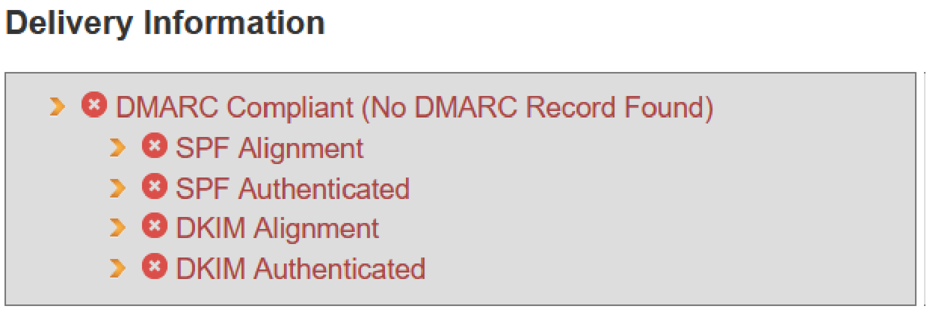
Email Header Analyzer

Paste Header:

```
Delivered-To:
Received: by 2002:ac0:d541:0:0:0:0:0 with SMTP id p1csp4116462imh;
        Tue, 1 Jun 2021 07:09:38 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJzbuGp/zKW5gwhBymf27M47Mvwke81vrltjFF0kC3ghdNaxG
X-Received: by 2002:a17:90a:aa94:: with SMTP id l20mr70487pjq.125.1622556578467;
        Tue, 01 Jun 2021 07:09:38 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1622556578; cv=none;
        d=google.com; s=arc-20160816;
        b=ZXpuhwFq+CPvPRcVSCfzfjvW3sc7YA/ao2sGEMU4LqEvoLuSulvkV4hLoXx8K4llXe
         3zYBK38xem2rCYwPJVi7r0ylKji89Fnlvlu7PwYx6JZQh5Gzn3UZ31tOpg8Mjp9akL22
         h0nzvMpMyDn5S5QJeDelQlzp+/Tmx2XSm/PmgnktpD7eZ7vkDNPsPaynozLoVlGhevlF
```

The MXToolbox Header Analysis tool breaks up the email header into smaller, manageable chunks.

Starting at the top of the results, we get a summary of the delivery information.



Delivery Information

- ⊗ DMARC Compliant (No DMARC Record Found)
  - ⊗ SPF Alignment
  - ⊗ SPF Authenticated
  - ⊗ DKIM Alignment
  - ⊗ DKIM Authenticated

To pass DMARC authentication, a message must both Pass and Align for either SPF or DKIM. Even if a message passed authentication for both SPF and DKIM, it could still fail DMARC authentication if one of them does not “align” with the sender’s policy.

If SPF Passes, the message was delivered from an IP address published in the SPF policy of the SMTP envelope “mail from:” (mfrom) domain, and if the DKIM Passes, the message was correctly signed by the d= domain in the DKIM header.

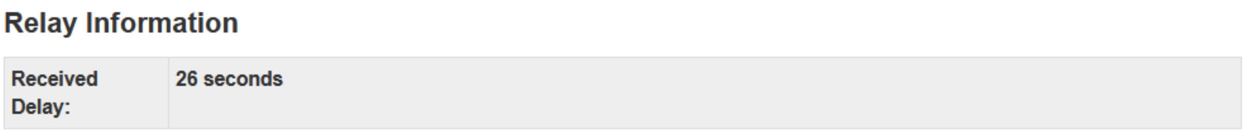
DKIM Aligns, means the <From:> header visible to the recipient matches the d= domain in the DKIM header.

SPF Aligns, means the <From:> header visible to the recipient matches the domain used to authenticate SPF. (e.g., the envelope “mail from:” domain)

When a message is aligned, the email recipient knows from which domain the message originated from.

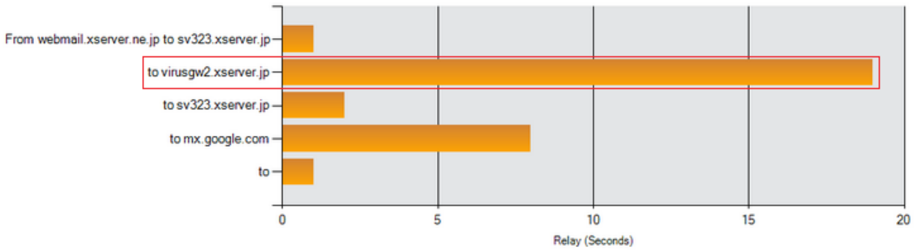
SPF and DKIM are only authentication mechanisms. Passing SPF or DKIM authentication only means the receiving organization can identify the actual sending domain. But typically, the end-user receiving the message never sees this domain. Instead, they see the “From:” address in the email header.

A message can pass both SPF and DKIM authentication and trick the end-user into thinking it came from someone else (i.e., spoofing). When a message is aligned, the friendly domain visible in the email client matches the domain used to authenticate with SPF or DKIM.



Relay Information

Received Delay:	**26 seconds**



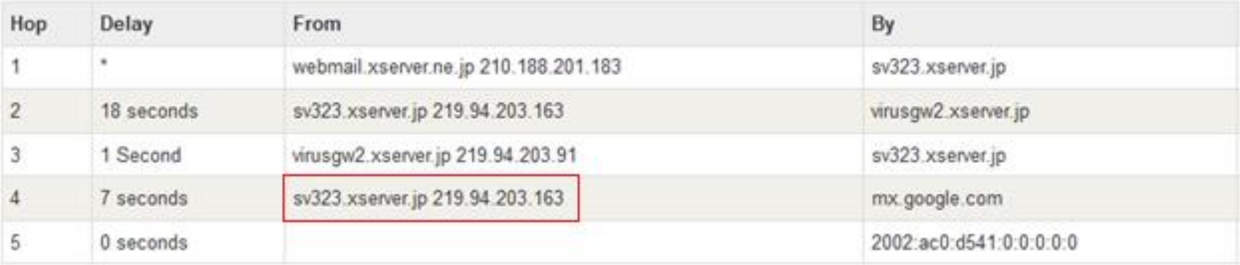
Each time a server relay receives an SMTP message, it will add a new Received: line at the beginning of the header block. A typical email received by a user on a corporate network will show many server relays both before and after being delivered to the corporate email servers (companyserver.com). These will be in chronological order starting from the bottom up.

By analyzing the server relay information in chronological order from the bottom-up, you can get a picture of where the message traveled. Each receiving mail server adds the name and IP address of the server that delivered the message. The server name may reveal the domain of the sender relay.

In the case of messages sent via Gmail and other large email service providers, this may only lead you back to the location of the email servers or even the corporate headquarters of the provider.

If you are lucky, the headers will include an X-Originating-IP that may reveal the sender's internet service provider and narrow down the sender's location.

In the following image, we see the relay information starting at the bottom with the name and IP address of the sending mail server.

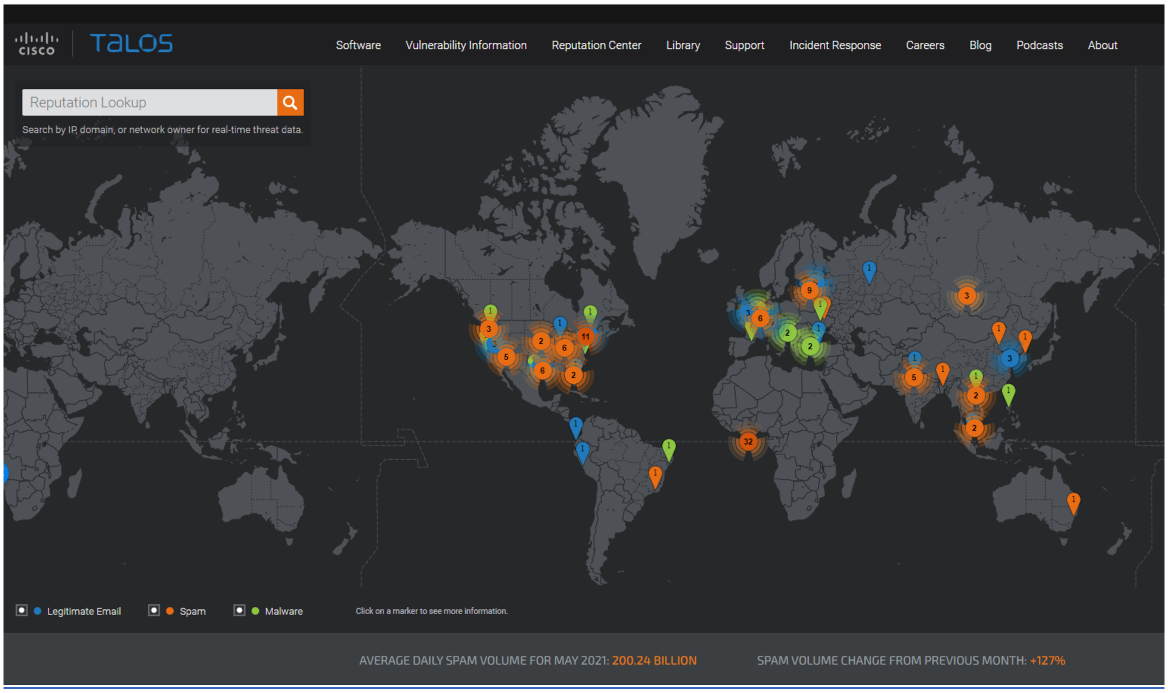


Hop	Delay	From	By
1	*	webmail.xserver.ne.jp 210.188.201.183	sv323.xserver.jp
2	18 seconds	sv323.xserver.jp 219.94.203.163	virusgw2.xserver.jp
3	1 Second	virusgw2.xserver.jp 219.94.203.91	sv323.xserver.jp
4	7 seconds	sv323.xserver.jp 219.94.203.163	mx.google.com
5	0 seconds		2002:ac0:d541:0:0:0:0:0

If you are looking at spam email headers from a network security perspective, it is important to identify the IP address/domain that delivered the email to your email server.

Verify the server's reputation

To verify the reputation of a domain, you can use a free reputation service such as the one provided by Cisco https://www.senderbase.org/



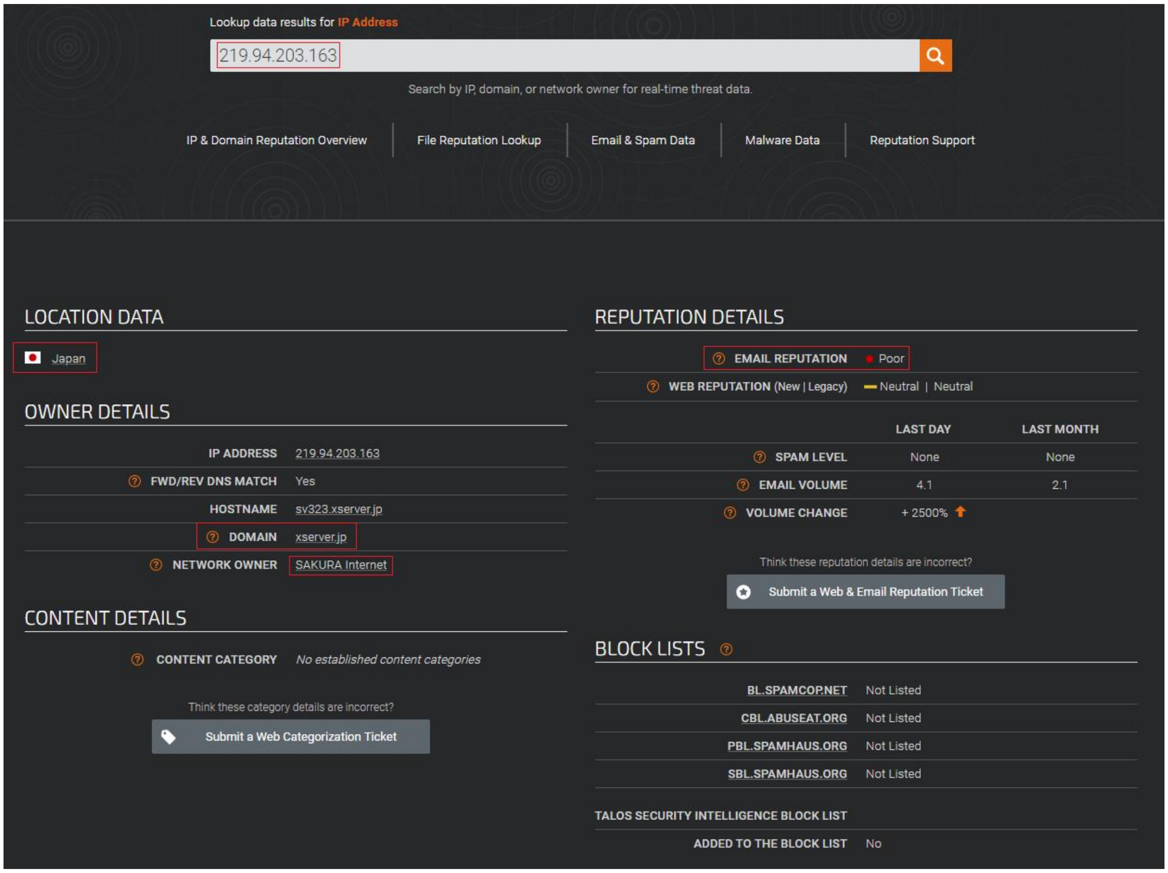
Search by IP, domain, or network owner for real-time threat data.

Click on a marker to see more information.

AVERAGE DAILY SPAM VOLUME FOR MAY 2021: 200.24 BILLION

SPAM VOLUME CHANGE FROM PREVIOUS MONTH: +127%

From our relay results, we see there is a server with a hostname of **server sv323.xserver.jp** using an IP address of **219.94.203.163**. Using the Cisco Talos site, we can check the reputation of the server.



Lookup data results for IP Address

219.94.203.163

Search by IP, domain, or network owner for real-time threat data.

LOCATION DATA

Japan

OWNER DETAILS

IP ADDRESS	219.94.203.163
FWD/REV DNS MATCH	Yes
HOSTNAME	sv323.xserver.jp
DOMAIN	xserver.jp
NETWORK OWNER	SAKURA Internet

CONTENT DETAILS

CONTENT CATEGORY *No established content categories*

Think these category details are incorrect?

Submit a Web Categorization Ticket

REPUTATION DETAILS

EMAIL REPUTATION ● Poor

WEB REPUTATION (New | Legacy) — Neutral | Neutral

	LAST DAY	LAST MONTH
SPAM LEVEL	None	None
EMAIL VOLUME	4.1	2.1
VOLUME CHANGE	+ 2500% ↑	

Think these reputation details are incorrect?

Submit a Web & Email Reputation Ticket

BLOCK LISTS

BL.SPAMCOP.NET	Not Listed
CBL.ABUSEAT.ORG	Not Listed
PBL.SPAMHAUS.ORG	Not Listed
SBL.SPAMHAUS.ORG	Not Listed

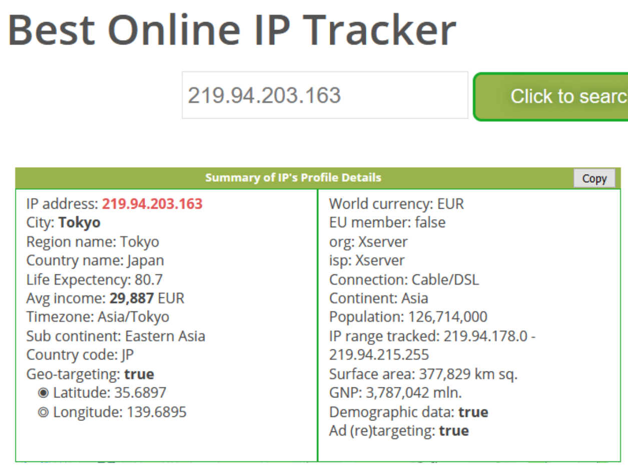
TALOS SECURITY INTELLIGENCE BLOCK LIST

ADDED TO THE BLOCK LIST No

We are trying to confirm the identity of the sender. So far, it does not look good. It is obvious that someone is posing as Dennis Olisa. So far, we know that reputation of the sending server is bad, and the email originated in Japan.

IP locators

The Internet has dozens if not hundreds of free IP locator sites. They all have different features and return different results. I like the features of Opentracker.net. It returns plenty of information about the IP address, but it also allows you to pinpoint the IP address location using satellite imaging and mapping.



Best Online IP Tracker

219.94.203.163 | Click to search!

Summary of IP's Profile Details | Copy

IP address: 219.94.203.163
City: **Tokyo**
Region name: Tokyo
Country name: Japan
Life Expectency: 80.7
Avg income: **29,887** EUR
Timezone: Asia/Tokyo
Sub continent: Eastern Asia
Country code: JP
Geo-targeting: **true**
◉ Latitude: 35.6897
◎ Longitude: 139.6895

World currency: EUR
EU member: false
org: Xserver
isp: Xserver
Connection: Cable/DSL
Continent: Asia
Population: 126,714,000
IP range tracked: 219.94.178.0 - 219.94.215.255
Surface area: 377,829 km sq.
GNP: 3,787,042 mln.
Demographic data: **true**
Ad (re)targeting: **true**

In this example, I can see where the device assigned the IP address **219.94.203.163** is located.

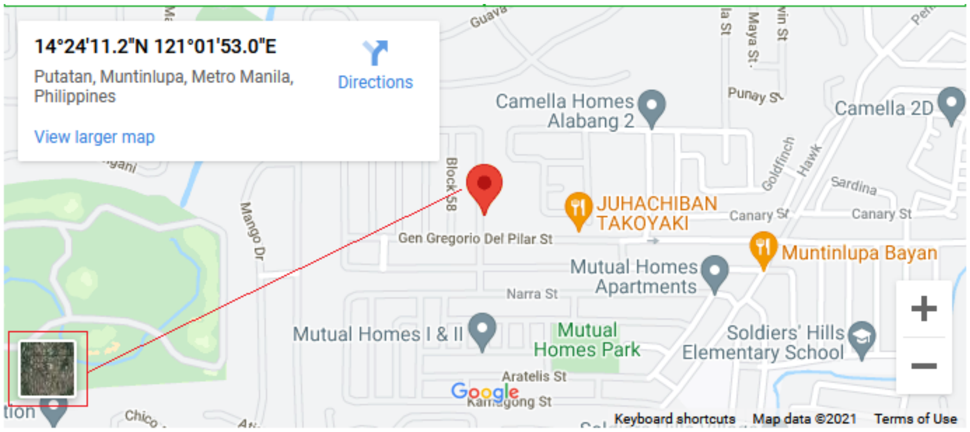
In our Google map, I have a red pin showing the server's location somewhere in Tokyo. By using Google Earth, I can see where the server is located.

Locating the IP address of the sender

If the stars and the planets are all aligned correctly, you may be able to see the originating IP address located in the email header. Not always, but it’s still worth investigating. Here is an example of what you might look for.

```
Received: from User (175.176.45.152) by mailgw2.stj-sin.gob.mx
(192.168.220.120) with Microsoft SMTP Server id 15.1.2242.4; Wed, 2 Jun 2021
21:28:24 -0600
```

Doing an IP lookup on this IP address takes me right to the sender’s rooftop. If I click on the icon to view the satellite image of the location, I am shown all the information I need to find the sender’s location.

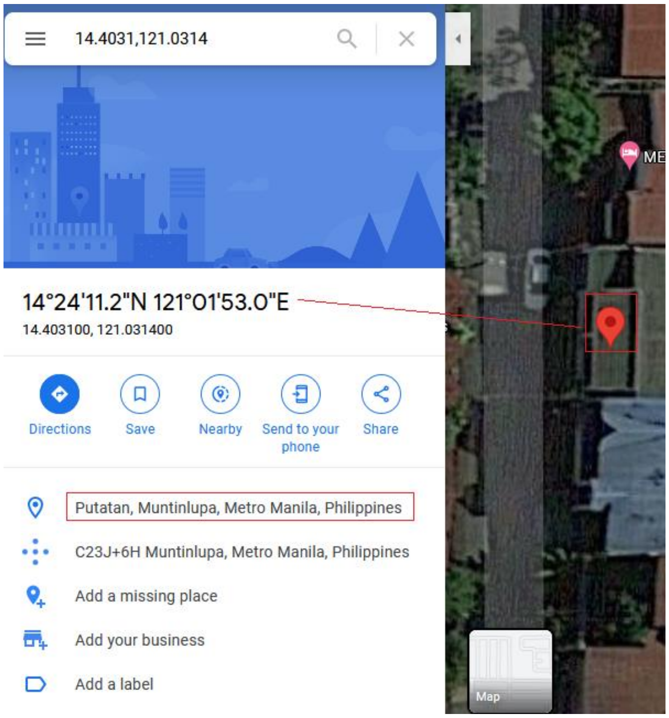


14°24'11.2"N 121°01'53.0"E

Putatan, Muntinlupa, Metro Manila, Philippines

View larger map

Satellite image as seen in the larger window.



14.4031,121.0314

14°24'11.2"N 121°01'53.0"E

14.403100, 121.031400

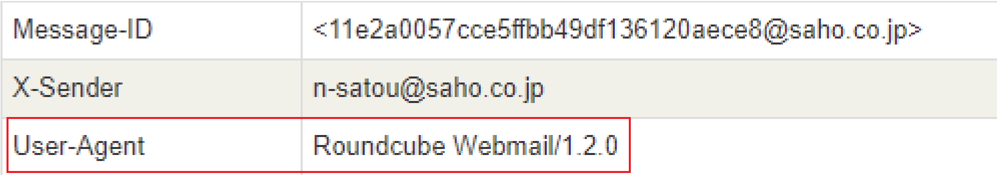
Putatan, Muntinlupa, Metro Manila, Philippines

C23J+6H Muntinlupa, Metro Manila, Philippines

If law enforcement were looking for this individual, they could input the coordinates into their GPS device and be taken to the person's front door. Granted, the location may be a church or the sender's neighbors' Wi-Fi but were in the vicinity. By looking at the log files of the access point, we would be able to see the actual IP address of the sender.

Follow the breadcrumbs

One thing that piqued my interest was the commonality that some spammers have. Down at the bottom of the email, you can see the user agent used to send the email.



Message-ID	<11e2a0057cce5ffbb49df136120aece8@saho.co.jp>
X-Sender	n-satou@saho.co.jp
User-Agent	Roundcube Webmail/1.2.0

Roundcube Webmail is a small open-source mail server application that could easily run on a laptop. The program needs an installation of IIS or Apache and MySQL database. I can imagine someone sitting at a table in a bakery in Tokyo connected to a free wireless network using their laptop to send out SPAM or malicious emails.

You see this program being used a lot by spammers.

No one does it better than the Russians

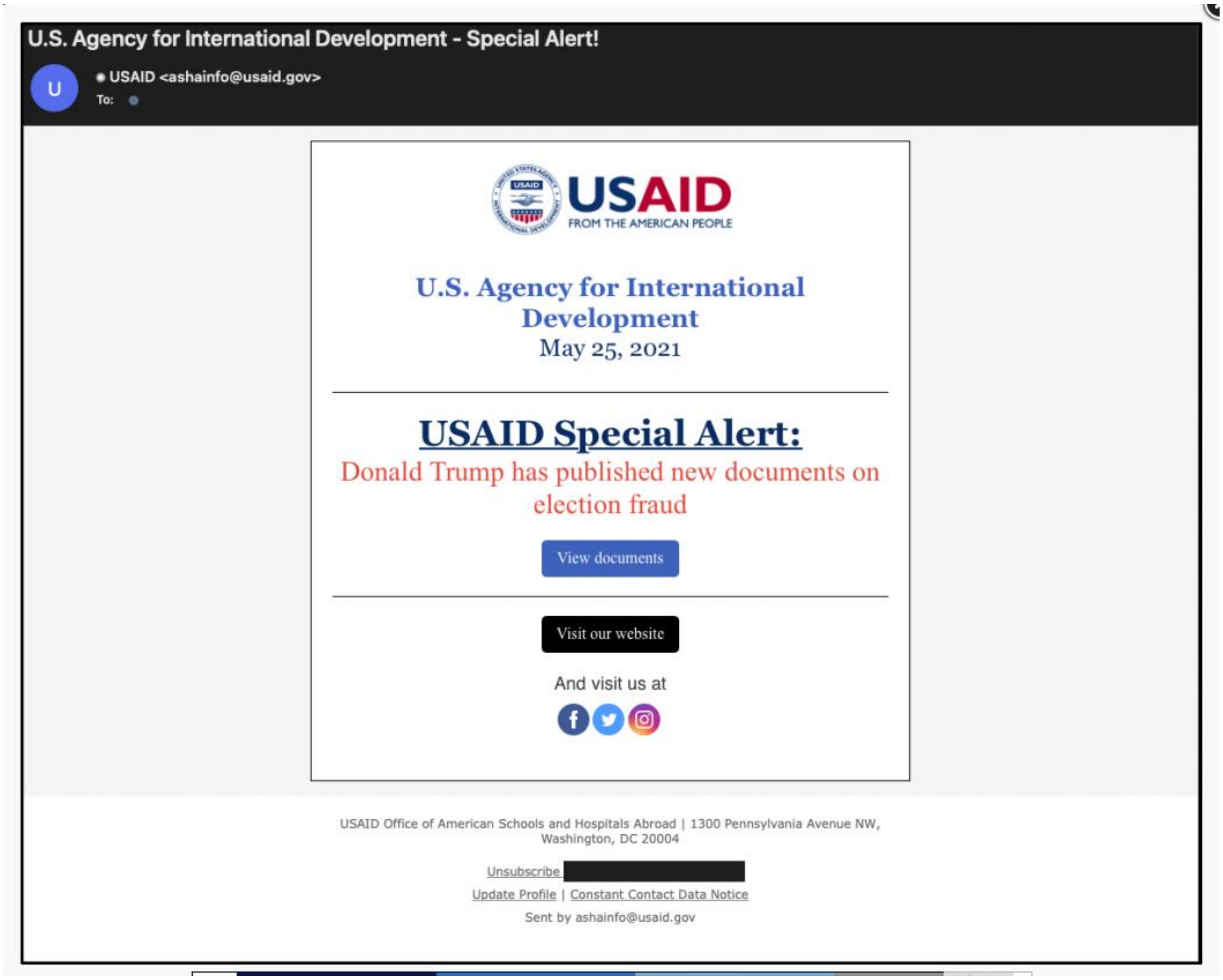
This recent malicious email sent to USIAD employees contained no fewer than four different malicious payloads. Love them or hate them; you must admire the craftsmanship that went into making this message. The message content pushes all the right buttons, and it uses the same message template that USAID uses when emailing their workers.

This message slipped right through the State Department filters. Those that clicked on the link to view the documents were immediately infected.

New malware used by Nobelium

In a second blog post released by Microsoft, Microsoft provides details on four new malware families used by Nobelium in recent attacks.

The four new families include an HTML attachment named 'EnvyScout,' a downloader known as 'BoomBox,' a loader known as 'NativeZone,' and a shellcode downloader and launcher named 'VaporRage.'



U.S. Agency for International Development - Special Alert!

USAID <ashainfo@usaid.gov>

To:

USAID
FROM THE AMERICAN PEOPLE

U.S. Agency for International Development
May 25, 2021

USAID Special Alert:

Donald Trump has published new documents on election fraud

And visit us at

USAID Office of American Schools and Hospitals Abroad | 1300 Pennsylvania Avenue NW,
Washington, DC 20004

Unsubscribe [redacted]
Update Profile | Constant Contact Data Notice
Sent by ashainfo@usaid.gov

This group is tracked as Nobelium (Microsoft), NC2452 (FireEye), StellarParticle (CrowdStrike), SolarStorm (Palo Alto Unit 42), and Dark Halo (Volexity).

Reference

https://www.bleepingcomputer.com/news/security/microsoft-russian-hackers-used-4-new-malware-in-usaid-phishing/

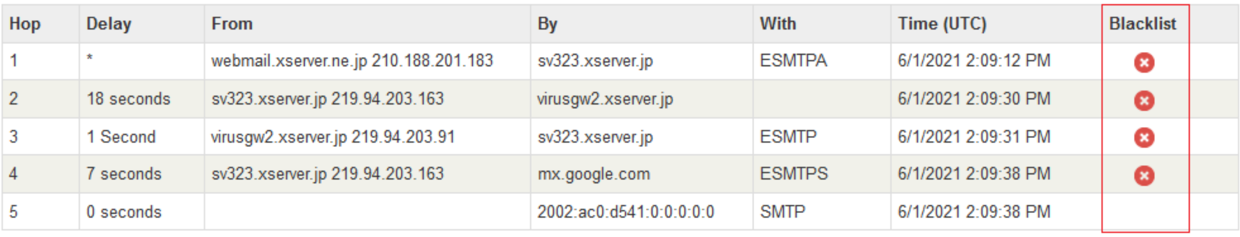
Analysis of the email

The security firm Volexity analyzed the message. You can read their analysis using this link.
Suspected APT29 Operation Launches Election Fraud Themed Phishing Campaigns

Well worth the read!

Blacklisting

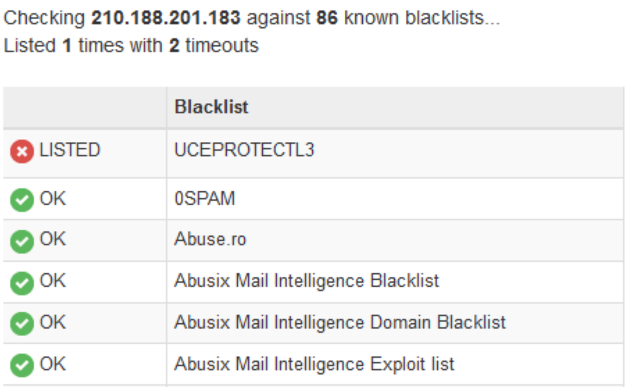
A blacklist is a real-time list that identifies IP addresses or domains that are known to send spam. They are used by organizations like internet service providers (ISPs), free mailbox providers, and anti-spam vendors to prevent spam from coming into their systems.



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	webmail.xserver.ne.jp 210.188.201.183	sv323.xserver.jp	ESMTPA	6/1/2021 2:09:12 PM	✖
2	18 seconds	sv323.xserver.jp 219.94.203.163	virusgw2.xserver.jp		6/1/2021 2:09:30 PM	✖
3	1 Second	virusgw2.xserver.jp 219.94.203.91	sv323.xserver.jp	ESMTP	6/1/2021 2:09:31 PM	✖
4	7 seconds	sv323.xserver.jp 219.94.203.163	mx.google.com	ESMTPS	6/1/2021 2:09:38 PM	✖
5	0 seconds		2002:ac0:d541:0:0:0:0:0	SMTP	6/1/2021 2:09:38 PM	

Blacklisting is not always an accurate indicator of a fake email. Some email providers will allow end-users to mark an email as SPAM. Suppose enough recipients subscribed to the same email provider mark the same sender as SPAM; the sender's IP address listed on their MX DNS record is blacklisted by the blacklisting service used by the email provider.

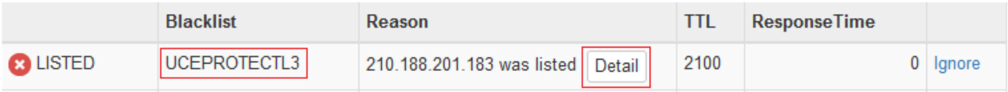
ISPs reuse their blocks of IP addresses. If a blacklisted IP address from a previous subscriber is given to a new prescriber, that new subscriber will also be blacklisted.



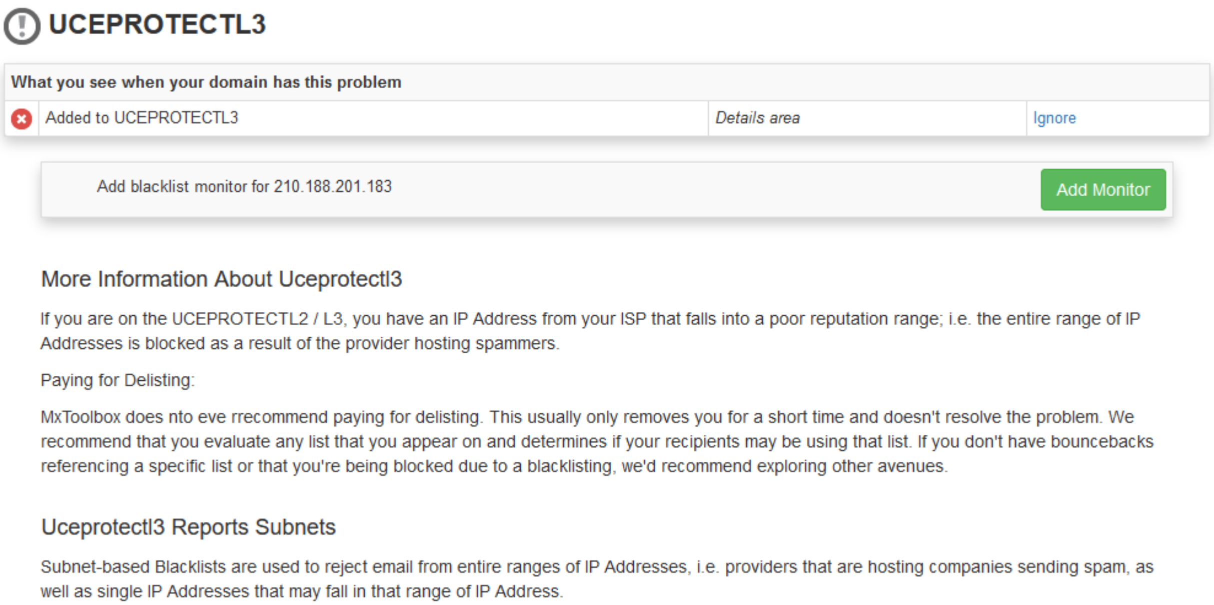
Checking **210.188.201.183** against **86** known blacklists...
Listed **1** times with **2** timeouts

	Blacklist
✖ LISTED	UCEPROTECTL3
✓ OK	0SPAM
✓ OK	Abuse.ro
✓ OK	Abusix Mail Intelligence Blacklist
✓ OK	Abusix Mail Intelligence Domain Blacklist
✓ OK	Abusix Mail Intelligence Exploit list

During the analysis, you can get more information about the Blacklisting service and why the IP address was blacklisted.



	Blacklist	Reason	TTL	ResponseTime	
✖ LISTED	UCEPROTECTL3	210.188.201.183 was listed Detail	2100	0	Ignore



UCEPROTECTL3

What you see when your domain has this problem			
✖	Added to UCEPROTECTL3	*Details area*	Ignore

Add blacklist monitor for 210.188.201.183

More Information About Uceprotectl3

If you are on the UCEPROTECTL2 / L3, you have an IP Address from your ISP that falls into a poor reputation range; i.e. the entire range of IP Addresses is blocked as a result of the provider hosting spammers.

Paying for Delisting:

MxToolbox does nto eve rrecommend paying for delisting. This usually only removes you for a short time and doesn't resolve the problem. We recommend that you evaluate any list that you appear on and determines if your recipients may be using that list. If you don't have bouncebacks referencing a specific list or that you're being blocked due to a blacklisting, we'd recommend exploring other avenues.

Uceprotectl3 Reports Subnets

Subnet-based Blacklists are used to reject email from entire ranges of IP Addresses, i.e. providers that are hosting companies sending spam, as well as single IP Addresses that may fall in that range of IP Address.

Summary –

In this lesson, we looked at analyzing email headers when trying to validate the authenticity of an email. You may need to identify the originating domain and IP address to prevent any messages from reaching your corporate users. It could be a threatening email sent to you or someone you care about. An email header can be a great source of digital information to locate the originating IP of the sender.