How to Trace an IP Address From an Email Explained

Posted on December 28, 2019

Ever felt the need to see what's happening with the recipient after you sent an email? You may have. In this post, we'll look at how email tracing is done for different email service providers as well as explore the reasons why you might find it useful.

How Email Tracing Works, in a Nutshell

Email tracing refers to the process of finding out what actions a recipient performed after getting an email such as when he or she opened or read it. Email tracing also lets senders know if intended recipients clicked on embedded links or downloaded attachments.

Most email service providers allow account owners to trace emails through IP addresses. This feat is accomplished with the simple addition of a single-pixel GIF to an email using the following code:

```
<img src="https://www.targetdomain.com/singlepixel.php" />
```

When a user wants to know when a recipient has read his email, the following code is added to the email. This creates or returns a single-pixel GIF on a request or web beacon:

```
<?php

echo base64_decode("R0lGODlhAQABAIAAAAAAAAAAACH5BAEAAAAALAAAAAABAAEAAAICRA

?>
```

Users can then employ a terminal or a shell (e.g., sendmail cmd) on a previously configured mail server to send traceable emails. As proof of concept (PoC), define the content file (i.e.,

content.html) in this manner:

```
From:
To: <target email>
Subject: Tracking Test Email
Mime-Version: 1.0
Content-Type: text/html

<h1>Test email</h1>
The body.
<img src=" https://www.targetdomain.com/singlepixel.php " />
```

Pipe this command afterward into sendmail by using the code:

```
$ cat content.html | sendmail -t
```

Every time a recipient gets an email and opens it, the email client gets the image link at least once. In some cases, a provider can cache this so the same image link is not triggered again.

Will this Work for All Email Clients?

The simple answer is it won't. Not all email clients support email tracing. Users can check if their clients' service provider does by sending an email and then monitoring their web server logs for receipt records (indicated by targetdomain.com in the PoC above).

In general, the majority of clients support email tracing, though at least 30% don't support IP-based email tracing (i.e., getting images via proxies).

We took a look at whether the most used services enable email tracing. Here are the codes we used:

- **Gmail:** Used by 29% of the total number of email service users surveyed in September of 2019.

```
66.249.81.157 - - [21/Sep/2019:21:01:36 +0000] "GET /singlepixel.php HTTP/1.1" 200 61 "-" "Mozilla/
```

Note that 66.249.81.157 is not the user's actual IP address. It is Google's IP address, which means the provider uses a proxy to fetch a remote image (i.e., GoogleImageProxy), thus preventing us from getting the recipient's correct IP address.

- **iPhone Apple Mail:** Used by 26% of the survey respondents.

```
xxx.xxx.xxx.xxx - - [21/Sep/2019:21:11:43 +0000] "GET /singlepixel.php HTTP/2.0" 200 28298 "-" "Mo
```

xxx.xxx.xxx.xxx is the correct IP address of the target's iPhone, which means Mail allows email tracing.

- **Outlook:** Used by 11% of the total number of respondents.

```
207.180.xxx.xxx - - [21/Sep/2019:21:04:00 +0000] "GET /singlepixel.php HTTP/2.0" 200 150 "https://o
```

207.180.xxx.xxx is the correct IP address of the target's system, which means Outlook allowsemail tracing.

- **Yahoo! Mail:** Used by 6% of the total number of survey respondents.

212.82.108.87 - - [21/Sep/2019:21:08:28 +0000] "GET /singlepixel.php HTTP/1.1" 200 61 "-" "YahooM

212.82.108.87 is not a proper IP address. It is Yahoo!'s IP address. Like Google, Yahoo! uses proxies to fetch remote images (i.e., YahooMailProxy). As such, users would not be able to obtain the recipient's IP address.

- **Private clients:** Privately owned email clients (e.g., RainLoop) also disable email tracing by default. RainLoop, however, gives users the option to "Display external images" by explicitly approving their appearance via clicking. Users who do so may enable email tracing in this manner via special configuration using the code:

xxx.xxx.xxx.xxx - - [21/Sep/2019:21:13:48 +0000] "GET /test.php HTTP/2.0" 200 150 "https://www.dor

xxx.xxx.xxx.xxx is the correct IP address of the target's system.

Why Would You Want to Trace Emails?

Now that we've talked about how it's possible in some cases to trace emails, let's see some of the reasons why you may want to do so:

Cybersecurity

Security researchers and law enforcement agents trace emails to learn more about threat actors involved in phishing, spamming, and other cyber attacks. Emails are, after all, the most commonly used means of entry into target networks. Cyber attackers need only use convincing social engineering lures to trick unsuspecting employees into opening ransomware- or other malware-laced emails; or send money to their accounts while posing as company executives.

By validating the safety of an email address, security professionals can proactively avoid malware infections and fraud. They can block email addresses contained in blacklists, so messages from these won't even reach their target inboxes.

Marketing

Email marketing is a proven way to communicate with potential customers. It has been said to yield US$44 for every dollar spent. Then again, marketers need to avoid ending up on email spamming lists by making sure they have low bounce rates.

One way of ensuring that messages are actually read and opened instead of marked as spam (which could lead to ending up in a blacklist) is by enabling email tracing. Recipients who don't open or read your emails can be taken off mailing lists to keep bounce rates low and thus avoid becoming part of an email blacklist.

Research

Conducting face-to-face interviews can be time-consuming and costly, which is why plenty of research organizations today opt to conduct email surveys instead. With it, they avoid the hassle

of setting up appointments and transportation costs. In some ways, they also get more detailed information from respondents.

In the research field, email tracing would hasten the process of checking which recipients actually responded to a survey. It could also simplify identifying who to re-send the questionnaires to or looking for alternative recipients should a pre-identified number of respondents be required for a particular industry.

Email tracing is an excellent means to find out if the intended recipients got your message. Tracing email addresses back to IP addresses generates more information on attackers in the field of cybersecurity, potential customers in marketing, and survey respondents in research. Protecting your organization from threats, knowing your market, and reaching contacts ensure not only safety from attacks but also business success.