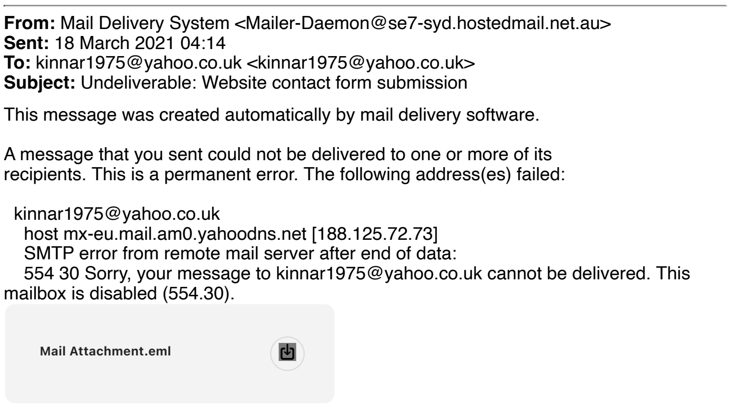
Phishing Email Analysis Report



From: Mail Delivery System <Mailer-Daemon@se7-syd.hostedmail.net.au>
Sent: 18 March 2021 04:14
To: kinnar1975@yahoo.co.uk <kinnar1975@yahoo.co.uk>
Subject: Undeliverable: Website contact form submission

This message was created automatically by mail delivery software.

A message that you sent could not be delivered to one or more of its
recipients. This is a permanent error. The following address(es) failed:

```
  kinnar1975@yahoo.co.uk
    host mx-eu.mail.am0.yahoodns.net [188.125.72.73]
    SMTP error from remote mail server after end of data:
    554 30 Sorry, your message to kinnar1975@yahoo.co.uk cannot be delivered. This
mailbox is disabled (554.30).
```

Potential Spam Email

1. Sender and Recipient Information

- **Primary Recipient Email Address: kinnar1975@yahoo.co.uk**
- **Originating IP Address:** 103.9.171.10
- **Resolved Host:** c5s2-1e-syd.hosting-services.net.au (based on reverse DNS lookup)

2. Email Content

- **Subject Line:** Website contact form submission
- **Date and Time Sent:** 18 March 2021 04:14

3. Technical Details

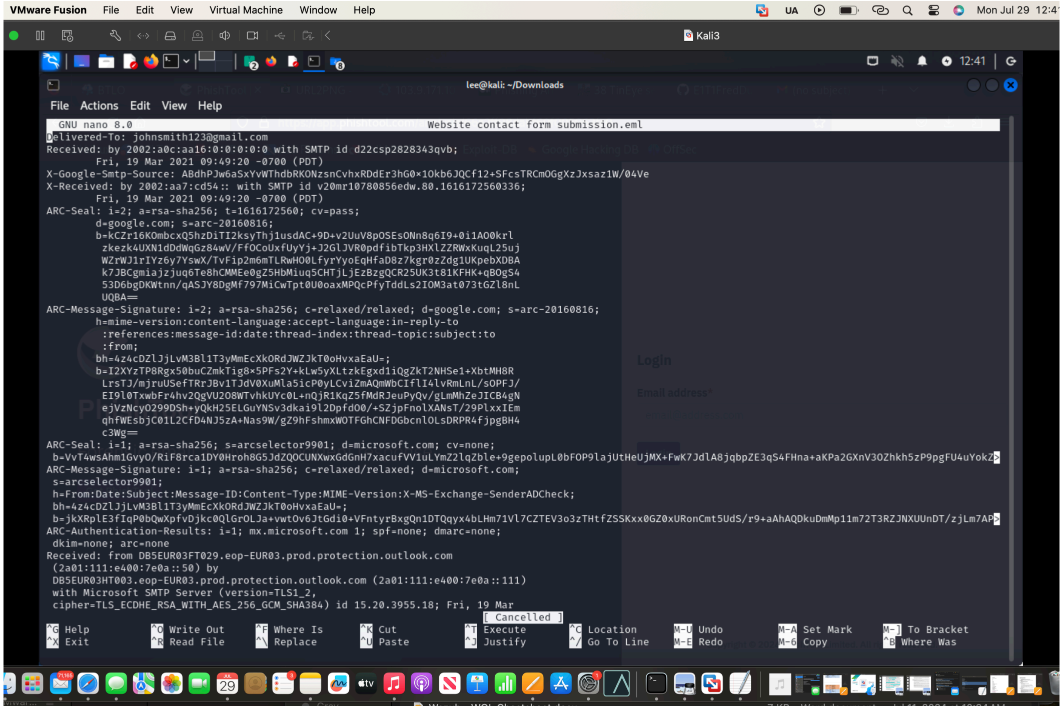
- **Attached File Name:** Website contact form submission
- **URL Found in Attachment:**
  - `https://35000usdperwwekpodf.blogspot.sg?p=9swg`
  - `https://35000usdperwwekpodf.blogspot.co.il?o=0hnd`
    `Both URLs use the Blogspot service.`
- **Webpage Heading Text:** When attempting to load the webpage, the message displayed is: "Webpage not found."

4. Phishing Indicators

- **Suspicious Originating IP:** The IP `103.9.171.10` is associated with a hosting service (`c5s2-1e-syd.hosting-services.net.au`) rather than a legitimate business domain, which is often used by attackers.
- **Suspicious URLs:** The URLs provided in the attachment lead to a Blogspot domain with unusual names and parameters, which are red flags for phishing attempts. Blogspot is a common platform for hosting malicious content.
- **Webpage Not Found:** The webpage associated with the URLs returns a "Webpage not found" message, indicating that the page might have been taken down, but it still poses a risk if it were active previously.

5. Conclusion

This email is a phishing attempt, leveraging suspicious URLs and an attachment that leads to potentially malicious content hosted on Blogspot. The use of a hosting service IP address and the failed webpage load are strong indicators of malicious intent. Recipients should not interact with any links or attachments in this email and should report it as phishing.



```
  GNU nano 8.0                                    Website contact form submission.eml
Delivered-To: johnsmith123@gmail.com
Received: by 2002:a0c:aa16:0:0:0:0:0 with SMTP id d22csp2828343qvb;
        Fri, 19 Mar 2021 09:49:20 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJw6aSxYvWThdbRKONzsnCvhxRDdEr3hG0×1Okb6JQCf12+SFcsTRCmOGgXzJxsaz1W/04Ve
X-Received: by 2002:aa7:cd54:: with SMTP id v20mr10780856edw.80.1616172560336;
        Fri, 19 Mar 2021 09:49:20 -0700 (PDT)
ARC-Seal: i=2; a=rsa-sha256; t=1616172560; cv=pass;
        d=google.com; s=arc-20160816;
        b=kCZr16KOmbcxQ5hzDiTI2ksyThj1usdAC+9D+v2UuV8pOSEsONn8q6I9+0i1AO0krl
         zkezk4UXN1dDdWqGz84wV/FfOCoUxfUyYj+J2GlJVR0pdfibTkp3HXlZZRWxKuqL25uj
         WZrWJ1rIYz6y7YswX/TvFip2m6mTLRwHO0LfyrYyoEqHfaD8z7kgr0zZdg1UKpebXDBA
         k7JBCgmiajzjuq6Te8hCMMEe0gZ5HbMiuq5CHTjLjEzBzgQCR25UK3t81KFHK+qBOgS4
         53D6bgDKWtnn/qASJY8DgMf797MiCwTpt0U0oaxMPQcPfyTddLs2IOM3at073tGZl8nL
         UQBA==
ARC-Message-Signature: i=2; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=mime-version:content-language:accept-language:in-reply-to
         :references:message-id:date:thread-index:thread-topic:subject:to
         :from;
        bh=4z4cDZlJjLvM3Bl1T3yMmEcXkORdJWZJkT0oHvxaEaU=;
        b=I2XYzTP8Rgx50buCZmkTig8×5PFs2Y+kLw5yXLtzkEgxd1iQgZkT2NHSe1+XbtMH8R
         LrsTJ/mjruUSefTRrJBv1TJdV0XuMla5icP0yLCviZmAQmWbCIflI4lvRmLnL/sOPFJ/
         EI9l0TxwbFr4hv2QgVU2O8WTvhkUYc0L+nQjR1KqZ5fMdRJeuPyQv/gLmMhZeJICB4gN
         ejVzNcyO299DSh+yQkH25ELGuYNSv3dkai9l2DpfdO0/+SZjpFnolXANsT/29PlxxIEm
         qhfWEsbjC01L2CfD4NJ5zA+Nas9W/gZ9hFshmxWOTFGhCNFDGbcnlOLsDRPR4fjpgBH4
         c3Wg==
ARC-Seal: i=1; a=rsa-sha256; s=arcselector9901; d=microsoft.com; cv=none;
 b=VvT4wsAhm1GvyO/RiF8rca1DY0Hroh8G5JdZQOCUNXwxGdGnH7xacufVV1uLYmZ2lqZble+9gepolupL0bFOP9lajUtHeUjMX+FwK7JdlA8jqbpZE3qS4FHna+aKPa2GXnV3OZhkh5zP9pgFU4uYokZ>
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com;
 s=arcselector9901;
 h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck;
 bh=4z4cDZlJjLvM3Bl1T3yMmEcXkORdJWZJkT0oHvxaEaU=;
 b=jkXRplE3fIqP0bQwXpfvDjkc0QlGrOLJa+vwtOv6JtGdi0+VFntyrBxgQn1DTQqyx4bLHm71Vl7CZTEV3o3zTHtfZSSKxx0GZ0xURonCmt5UdS/r9+aAhAQDkuDmMp11m72T3RZJNXUUnDT/zjLm7AP>
ARC-Authentication-Results: i=1; mx.microsoft.com 1; spf=none; dmarc=none;
 dkim=none; arc=none
Received: from DB5EUR03FT029.eop-EUR03.prod.protection.outlook.com
 (2a01:111:e400:7e0a::50) by
 DB5EUR03HT003.eop-EUR03.prod.protection.outlook.com (2a01:111:e400:7e0a::111)
 with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3955.18; Fri, 19 Mar
                                                  [ Cancelled ]
^G Help          ^O Write Out     ^F Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo         M-A Set Mark     M-] To Bracket
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo         M-6 Copy         ^B Where Was
```