Phishing Investigation Report - BTLO

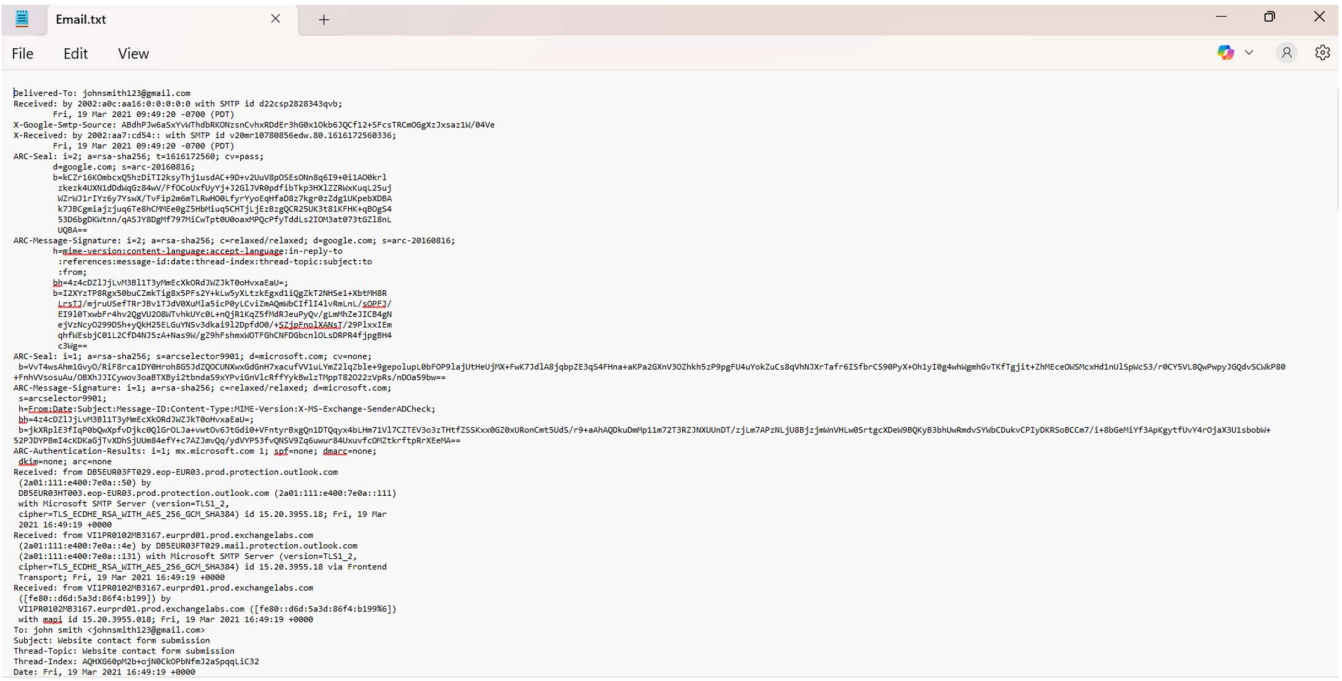
1. Overview

This report documents the analysis of a phishing email encountered during a BTLO (Blue Team Labs Online) challenge. The email included suspicious headers, malicious URLs, and misleading content. Multiple forensic tools were used in this investigation, including EML Analyzer, WHOIS lookup, manual header inspection, and phishing website preview capture.

2. Email Header Analysis

The email was received by johnsmith123@gmail.com and originated from markgard@c5s2-1e-syd.hosting-services.net.au. The IP address traced to 103.9.171.10, hosted in Australia. The header showed signs of spoofing, invalid sender domain, a disabled mailbox destination, and the presence of non-standard PHP-generated content. These red flags indicate potential malicious intent.

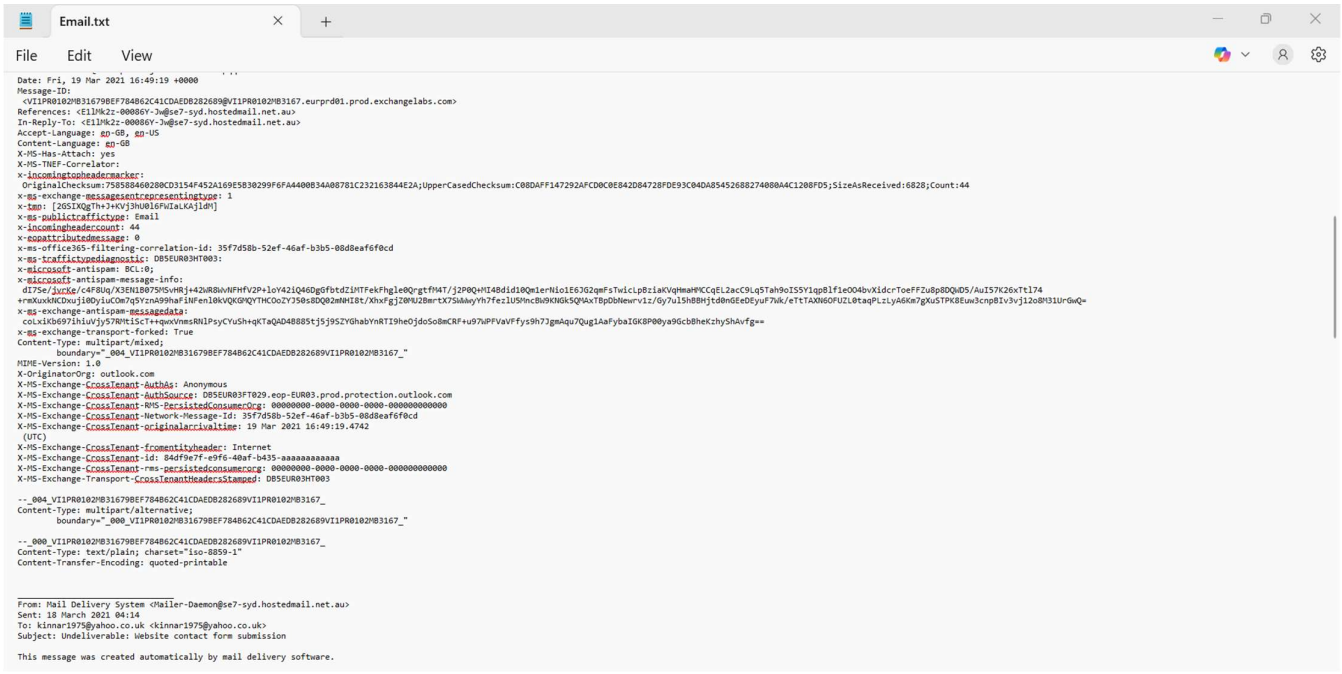
Phishing Investigation Report - BTLO



Email.txt

File Edit View

```
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: ABdhPJw6aSxYvWThdbRKONznsCvhxRDdEr3hG0x1Okb6JQCf12+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=kCZr16KOmbcxQ5hzDiT12ksyThj1usdAC+9D+v2UuV8pOSEsONn8q6I9+0i1AO0kr1
         zkezk4UXN1dDdhWqGz84wV/FfOCoUxfUyYj+J2GlJVR0pdfibTkp3HXlZZRkxKuqL25uj
         WZrW3lrIYz6y7YswK/TvFip2m6eTLRwHOOLfyrYyoEqHfaD8z7kgr0zIdg1UKpebXDBA
         k7J8CgmiajzjuqGTe8hCYMtEeBgZSHbH1uqSCHTjLjEz8zgQCR2SUK3t81KfMK+qBCgS4
         53D6bgDKWtnn/qASJYBDgMf797HiCwTptU0UoaxMPQcPfyTddLs2IOM3at073tGZl8nL
         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=4s4cD2l7jLvM3B1lT3yMmEcXkORdJWZJkT0oMvxaEaU=;
        b=I2XYzTP8Rgx50buCZmkTig8x5PFs2Y+kLw5yXLtzkEgxd1iQgZkT2NMSe1+XbtMHBR
         LrsTJ/mjruUSefTRrJBv1TJdV0XuMla5icP0yiCviZmAQmkbCIflI4lvRmLnL/sQPFJ/
         EI910TxwbFr4hv2QgVU2O8WTvhkUYc0L+nQjR1KqZ5fMdRJeuPyQv/gLmMhIeJICB4gN
         ejVzNcyO299O5h+yQkH25ELGuYN5v3dkaI9l2DpfdO0/+SZJpFnolXANsT/29PlxxIEm
         qhfuEsbjC0i1ZCfD4N35zA+Nas9W/g29HfshmxkOTfGhCNFOObcnlOLsDRPR4fjpgBH4
         c3Ug==
ARC-Seal: i=1; a=rsa-sha256; s=arcselector9901; d=microsoft.com; cv=none;
 b=VvT4wsAhm1OvyO/RiF8rca1DY0HrohBG5JdZQOCUNXwxGdGmH7xacufVV1uLYeZ2lqIble+9gepolupL0bFOP9lajUtHeUjMX+FwK7JdlA8jqbpZE3q54FHna+aKPa2GXnV3OZhkh5zP9pgFU4uYokZuCs8qVhNJXrTafr6ISfbrCS90PyX+Oh1yI0g4whWgmhGvTKfTgjit+ZhMEceOkSMcxHd1nUlSpWcS3/r0CY5VL8QwPwpyJGQdvSCwkP80
+fnhVVsosuAu/OBXDJJICywov3oaBTXBy12tbnda59xYPviGnVIcRffVykBwlzTMppT82O22tVpRs/nDOa59bw==
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=4z4cD2l7jLvM3B1lT3yMmEcXkORdJWZJkT0oMvxaEaU=;
 b=jkXRpIE3fIqP0bQwXpfvDjkc0QlGrOLJa+vwtOv67tGdi0+VFntyrBxgQn1DTQqyx4bLHm71Vl7CZTEV3o3zTHtfZSSKxx0GZ0xURonCmt5UdS/r9+aAhAQDkuDmMp11m72T3RZJNXUUnDT/zjLm7APzNLjU8BjrjmWnVHLw0SrtgcXDeW9BQKyB3bhUwRmdvSYWbCDukvCPIyDKRSoBCCm7/i+8bGeMiYf3ApKgytfUvY4rOjaX3U1sbobW+
52PJDYPBmI4cKDKaGjTvXDhSjUUm84efY+c7AZJmvQq/ydVYP53fvQNSV9Zq6uwur84UxuvfcOMZtkrftpRrXEeMA==
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
 2021 16:49:19 +0000
Received: from VI1PR0102MB3167.eurprd01.prod.exchangelabs.com
 (2a01:111:e400:7e0a::4e) by DB5EUR03FT029.mail.protection.outlook.com
 (2a01:111:e400:7e0a::131) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3955.18 via Frontend
 Transport; Fri, 19 Mar 2021 16:49:19 +0000
Received: from VI1PR0102MB3167.eurprd01.prod.exchangelabs.com
 ([fe80::d6d:5a3d:86f4:b199]) by
 VI1PR0102MB3167.eurprd01.prod.exchangelabs.com ([fe80::d6d:5a3d:86f4:b199%6])
 with mapi id 15.20.3955.018; Fri, 19 Mar 2021 16:49:19 +0000
To: john smith <johnsmith123@gmail.com>
Subject: Website contact form submission
Thread-Topic: Website contact form submission
Thread-Index: AQHXG60pM2b+ojN0CkOPbNfmJ2aSpqqLiC32
Date: Fri, 19 Mar 2021 16:49:19 +0000
```



Email.txt

File Edit View

```
Date: Fri, 19 Mar 2021 16:49:19 +0000
Message-ID:
 <VI1PR0102MB31679BEF784B62C41CDAEDB282689@VI1PR0102MB3167.eurprd01.prod.exchangelabs.com>
References: <E1lMk2z-00086Y-Jw@se7-syd.hostedmail.net.au>
In-Reply-To: <E1lMk2z-00086Y-Jw@se7-syd.hostedmail.net.au>
Accept-Language: en-GB, en-US
Content-Language: en-GB
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
x-incomingtopheadermarker:
 OriginalChecksum:758588460280CD3154F452A169E5B30299F6FA4400B34A08781C232163844E2A;UpperCasedChecksum:C08DAFF147292AFCD0C0E842D84728FDE93C04DA8545268827408 0A4C1208FD5;SizeAsReceived:6828;Count:44
x-ms-exchange-messagesentrepresentingtype: 1
x-tmn: [2GSIXQgTh+J+KVj3hU0l6FWIaLKAjldM]
x-ms-publictraffictype: Email
x-incomingheadercount: 44
x-eopattributedmessage: 0
x-ms-office365-filtering-correlation-id: 35f7d58b-52ef-46af-b3b5-08d8eaf6f0cd
x-ms-traffictypediagnostic: DB5EUR03HT003:
x-microsoft-antispam: BCL:0;
x-microsoft-antispam-message-info:
 dI75e/jvrKe/c4F8Uq/X3EN1B075MSvHRj+42wR8wVNFHfV2P+loY421Q46DgGfbtdZiMTFekFhgle0QrgtfM4T/j2P0Q+MI48did10Qm1erNio1E6JG2qmFsTwicLpBziaKVqHmaMMCCqEL2acC9Lq5Tah9oI55Y1qpBlf1eOO4bvXidcrToeFFZu8p8DQWD5/AuI57K26xTtl74
+rmXuxkNCDxuji0DyiuCOm7q5YznA99haFiNFenl0kVQKGMQYTHCOoZYJ5ds8DQ02mMXAxTBpDbNewrv1z/Gy7ul5hBBHjtd0nGEeDEyuF7Wk/eTtTAXN6OFUZL0taqPLzLyA6Km7gXuSTPK8Euw3cnpBIv3vji2o8M31UrGwQ=
x-ms-exchange-antispam-messagedata:
 coLx1kb697ihiuVjy57RMti5cT++qwxVnmsRNlPsyCYuShqKTaQAD4B885tj5j9SZYGhabYnRTI9heOjdoSo8mCRF+u97WPFVaVFfys9h7JgmAqu7Qug1AaFybaIGK8P00ya9GcbBheKzhyShAvfg==
x-ms-exchange-transport-forked: True
Content-Type: multipart/mixed;
        boundary="_004_VI1PR0102MB31679BEF784B62C41CDAEDB282689VI1PR0102MB3167_"
MIME-Version: 1.0
X-OriginatorOrg: outlook.com
X-MS-Exchange-CrossTenant-AuthAs: Anonymous
X-MS-Exchange-CrossTenant-AuthSource: DB5EUR03FT029.eop-EUR03.prod.protection.outlook.com
X-MS-Exchange-CrossTenant-RMS-PersistedConsumerOrg: 00000000-0000-0000-0000-000000000000
X-MS-Exchange-CrossTenant-Network-Message-Id: 35f7d58b-52ef-46af-b3b5-08d8eaf6f0cd
X-MS-Exchange-CrossTenant-originalarrivaltime: 19 Mar 2021 16:49:19.4742
 (UTC)
X-MS-Exchange-CrossTenant-fromentityheader: Internet
X-MS-Exchange-CrossTenant-id: 84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa
X-MS-Exchange-CrossTenant-rms-persistedconsumerorg: 00000000-0000-0000-0000-000000000000
X-MS-Exchange-Transport-CrossTenantHeadersStamped: DB5EUR03HT003

--_004_VI1PR0102MB31679BEF784B62C41CDAEDB282689VI1PR0102MB3167_
Content-Type: multipart/alternative;
        boundary="_000_VI1PR0102MB31679BEF784B62C41CDAEDB282689VI1PR0102MB3167_"

--_000_VI1PR0102MB31679BEF784B62C41CDAEDB282689VI1PR0102MB3167_
Content-Type: text/plain; charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable


_____

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.
```

Phishing Investigation Report - BTLO

```
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 delivere=
d. This mailbox is disabled (554.30).

--_000_VI1PR0102MB31679BEF784B62C41CDAEDB282689VI1PR0102MB3167_
Content-Type: text/html; charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

<html>
<head>
<meta http-equiv=3D"Content-Type" content=3D"text/html; charset=3Diso-8859-=
1">
<style type=3D"text/css" style=3D"display:none;"> P {margin-top:0;margin-bo=
ttom:0;} </style>
</head>
<body dir=3D"ltr">
<div style=3D"font-family: Calibri, Helvetica, sans-serif; font-size: 12pt;=
 color: rgb(0, 0, 0);">
<br>
</div>
<div>
<div id=3D"appendonsend"></div>
<hr tabindex=3D"-1" style=3D"display:inline-block; width:98%">
<div id=3D"divRplyFwdMsg" dir=3D"ltr"><font face=3D"Calibri, sans-serif" co=
lor=3D"#000000" style=3D"font-size:11pt"><b>From:</b> Mail Delivery System =
&lt;Mailer-Daemon@se7-syd.hostedmail.net.au&gt;<br>
<b>Sent:</b> 18 March 2021 04:14<br>
<b>To:</b> kinnar1975@yahoo.co.uk &lt;kinnar1975@yahoo.co.uk&gt;<br>
<b>Subject:</b> Undeliverable: Website contact form submission</font>
<div> </div>
</div>
<div class=3D"BodyFragment"><font size=3D"2"><span style=3D"font-size:11pt"=
>
<div class=3D"PlainText">This message was created automatically by mail del=
ivery software.<br>
<br>
A message that you sent could not be delivered to one or more of its<br>
recipients. This is a permanent error. The following address(es) failed:<br=
>
<br>
  kinnar1975@yahoo.co.uk<br>
    host mx-eu.mail.am0.yahoodns.net [188.125.72.73]<br>
    SMTP error from remote mail server after end of data:<br=
>
    554 30 Sorry, your message to kinnar1975@yahoo.co.uk can=
not be delivered. This mailbox is disabled (554.30).<br>
</div>
</span></font></div>
</div>
</body>
</html>
```

```
Received: from c5s2-1e-syd.hosting-services.net.au ([103.9.171.10])
        by se7-syd.hostedmail.net.au with esmtps (TLSv1.2:AES128-GCM-SHA256:128)
        (Exim 4.92)
        id 1lMk2r-0007vB-6O
        for kinnar1975@yahoo.co.uk; Thu, 18 Mar 2021 15:14:06 +1100
Received: from markgard by c5s2-1e-syd.hosting-services.net.au with local (Exim 4.94)
        id 1lMk2m-002w3b-NT
        for kinnar1975@yahoo.co.uk; Thu, 18 Mar 2021 15:13:56 +1100
To: kinnar1975@yahoo.co.uk
Subject: Website contact form submission
X-PHP-Script: www.markgardner.com.au/index.php for 91.90.123.43
X-PHP-Filename: /home/markgard/public_html/index.php REMOTE_ADDR: 91.90.123.43
Message-ID: <9af4091a6356d03e08c653d61c3317c5@www.markgardner.com.au>
Date: Thu, 18 Mar 2021 15:13:56 +1100
Content-Type: text/html; charset=utf-8
Content-Transfer-Encoding: quoted-printable
X-AntiAbuse: This header was added to track abuse, please include it with any abuse report
X-AntiAbuse: Primary Hostname - c5s2-1e-syd.hosting-services.net.au
X-AntiAbuse: Original Domain - yahoo.co.uk
X-AntiAbuse: Originator/Caller UID/GID - [645 501] / [47 12]
X-AntiAbuse: Sender Address Domain - hotmail.co.uk
X-Get-Message-Sender-Via: c5s2-1e-syd.hosting-services.net.au: authenticated_id: markgard/only user confirmed/virtual account not confirmed
X-Authenticated-Sender: c5s2-1e-syd.hosting-services.net.au: markgard
X-Source:
X-Source-Args:
X-Source-Dir: markgardner.com.au:/public_html
X-Originating-IP: 103.9.171.10
X-SpamExperts-Domain: out-2.hosting-services.net.au
X-SpamExperts-Username: 103.9.171.10
Authentication-Results: hostedmail.net.au; auth=pass smtp.auth=103.9.171.10@out-2.hosting-services.net.au
X-SpamExperts-Outgoing-Class: unsure
X-SpamExperts-Outgoing-Evidence: Combined (0.52)
X-Recommended-Action: accept
X-Filter-ID: Pt3HvcO5N4iKaDQ5O6lkdGlMVN6RH8bjRMzItlySaT89hY7QKxoN2bH3hJaGW2IpPUtbdvnXkggZ
 3YnVId/Y5jcf0yeVQAvfjHznO7+bT5zqUA8hT1A9YKB9i1C8tm0FSY5pAhCsHHyuxCwGLoOzBIJL
 M0i5ZAms0EHrvcCaVIMMGG9jpucc0SNLsDvCI1wozIXV52OyeiH3YVVX92r9xygFBqP9R4pweyxd
 HXGiL7j6BpeseSBELv+0jcKNeZXKhVuvOR3Ln3jZRs77DOT24JCTMkaicdLs0JYHIM966+y5TpWT
 FsQKCOuiS4S8pbsCwiF5chQ0eGHndnjZbM6wL3TaeQtlKubP6iUTjj6yPASOmrbMWhZFkvyjvYIF
 be8tdb9BwqvSI91oKEKHszPrHGllke3azHdKmySKNUVQl4ntlVxnbS8qIO7oudHyb2T1emsmnnq8
 H5RnRriVft+dRaZGawtRufZzJOZwa6OUbLspcvZoI7P90p8oLprk3TF7EVBannnL7tRRK/uB8nvA
 5dTkQHZZAFXxrDiK8BajMqIBbapBffof8ZbjRi48kxwwd/8g8ph5pmY3BWxh+gw0+bNud3PgzKGZ
 88iododq/YfVWMlHoWh7YJ70YBk8N5yx6J1fhOzjF0b4LXcjJZ5lophHcCCSZA0wo+GCaDbv8BVl
 BrgfA+nWs+ztZpIm+YUajlb62b+LvSOnVgYfMfV4/FZVYBSmXLV0H9UwfJB5VkyXuNsMOTPAVIrj
 2CQcJI3nLOjrOwwGI3kKu05JnDlv7nu+R5njOOVDeTnBQh+vgakM+3bjD6YI0Pi00Yp9Jo2PalvC
 Jx/RaFcuVNt8/inhvATugv1leQFvfCG5Mo+bZdrT9kO/rNfjYvuiOaQMP7hsYO4RKhzUPwqM4mnL
 vWdl6qmCT+WDVl7mMFEDbEvOkCuSUAX+wQaSOBQUHJ9fl0pktssFkv3lRh6UA/3FEjNcCz7Qn5mE
 3ifZ1Wx+Bxers9vSFjcXvojt6rPDFXmX7JFPjVZ28Fo80MP7MdFAR4SkjoOu+oaeH1BvSVyLTJZ2
 qqIBbapBffof8ZbjRi48kxwwEp0StAIU5onMW52eptt78P9RT6iLoaztK96skCBBmEn58PNKHent
 BN+4pS7z1zv6So+O6aenwaZ6/X2ea4ZBUw==
X-Report-Abuse-To: spam@se1-syd.hostedmail.net.au
MIME-Version: 1.0
```

3. WHOIS Domain Lookup

The WHOIS lookup shows that the IP 103.9.171.10 belongs to a commercial hosting provider. There is no legitimate business or organization associated with it, indicating that the address might be misused to host spam or phishing infrastructure.

Phishing Investigation Report - BTLO

DomainTools PROFILE CONNECT MONITOR SUPPORT Whois Lookup LOGIN Sign Up

Home > Whois Lookup > 103.9.171.10

Notice: Possible deprecation of Whois services after January 28, 2025. More Info

IP Information for 103.9.171.10

– Quick Stats

IP Location	Australia Sydney Synergy Wholesale Pty Ltd
ASN	AS45638 SYNERGYWHOLESALE-AP SYNERGY WHOLESALE PTY LTD, AU (registered Feb 23, 2009)
Resolve Host	c5s2-1e-syd.hosting-services.net.au
Whois Server	whois.apnic.net
IP Address	103.9.171.10
Reverse IP	6 websites use this address.


```
% Abuse contact for '103.9.168.0 - 103.9.171.255' is ' noc-abuse@nexigen.digital '

inetnum:        103.9.168.0 - 103.9.171.255
netname:        SYNERGYWHOLESALE-AP
descr:          SYNERGY WHOLESALE PTY LTD
descr:          Suite 105
descr:          66 Victor Crescent
descr:          Narre Warren VIC 3805
country:        AU
org:            ORG-SWPL1-AP
admin-c:        SWN3-AP
tech-c:         SWN3-AP
abuse-c:        AS2533-AP
status:         ASSIGNED PORTABLE
remarks:        ----------------------------------------------------------
remarks:        To report network abuse, please contact mnt-irt
remarks:        For troubleshooting, please contact tech-c and admin-c
remarks:        Report invalid contact via www.apnic.net/invalidcontact
remarks:        ----------------------------------------------------------
mnt-by:         APNIC-HM
mnt-routes:     MAINT-AU-SYNERGYWHOLESALE
mnt-irt:        IRT-SYNERGYWHOLESALE-AU
last-modified:  2020-07-08T00:57:37Z
source:         APNIC

irt:            IRT-SYNERGYWHOLESALE-AU
address:        PO Box 119
address:        Beaconsfield VIC 3807
address:        Australia
e-mail:         noc-general@nexigen.digital
abuse-mailbox:  noc-abuse@nexigen.digital
admin-c:        SWN3-AP
tech-c:         SWN3-AP
auth:           # Filtered
remarks:        noc-general@nexigen.digital was validated on 2025-01-03
remarks:        noc-abuse@nexigen.digital is invalid
mnt-by:         MAINT-AU-SYNERGYWHOLESALE
last-modified:  2025-04-02T13:07:44Z
source:         APNIC

organisation:   ORG-SWPL1-AP
org-name:       SYNERGY WHOLESALE PTY LTD
```

Phishing Investigation Report - BTLO

```
organisation:   ORG-SWPL1-AP
org-name:       SYNERGY WHOLESALE PTY LTD
org-type:       LIR
country:        AU
address:        PO BOX 119
phone:          +61-3-9013-8464
fax-no:         +61-3-8080-6481
e-mail:         noc-general@nexigen.digital
mnt-ref:        APNIC-HM
mnt-by:         APNIC-HM
last-modified:  2023-09-05T02:16:15Z
source:         APNIC

role:           ABUSE SYNERGYWHOLESALEAU
country:        ZZ
address:        PO Box 119
address:        Beaconsfield VIC 3807
address:        Australia
phone:          +000000000
e-mail:         noc-general@nexigen.digital
admin-c:        SWN3-AP
tech-c:         SWN3-AP
nic-hdl:        AS2533-AP
remarks:        Generated from irt object IRT-SYNERGYWHOLESALE-AU
remarks:        noc-general@nexigen.digital was validated on 2025-01-03
remarks:        noc-abuse@nexigen.digital is invalid
abuse-mailbox:  noc-abuse@nexigen.digital
mnt-by:         APNIC-ABUSE
last-modified:  2025-04-02T13:08:21Z
source:         APNIC

person:         Synergy Wholesale NOC
address:        PO BOX 119
                Beaconsfield VIC 3807
country:        AU
phone:          +61.390138464
fax-no:         +61.380806481
e-mail:         noc-general@nexigen.digital
nic-hdl:        SWN3-AP
notify:         noc-general@nexigen.digital
abuse-mailbox:  noc-abuse@nexigen.digital
mnt-by:         MAINT-AU-SYNERGYWHOLESALE
last-modified:  2021-09-27T01:25:35Z
source:         APNIC

route:          103.9.171.0/24
origin:         AS45638
descr:          SYNERGY WHOLESALE PTY LTD
                PO BOX 119
mnt-by:         MAINT-AU-SYNERGYWHOLESALE
last-modified:  2020-01-24T02:52:50Z
source:         APNIC
```

EML Analyzer Screenshots:

Phishing Investigation Report - BTLO

Headers

Basic headers

Message ID	<VI1PR0102MB31679BEF784B62C41CDAEDB282689@VI1PR0102MB3167.eurprd01.prod.exchangelabs.com>
Subject	Website contact form submission
Date (UTC)	2021-03-19T16:49:19Z
To	johnsmith123@gmail.com

Hops

Hop	From	By	With	Date (UTC)
1	vi1pr0102mb3167.eurprd01.prod.exchangelabs.com, fe80::d6d:5a3d:86f4:b199	vi1pr0102mb3167.eurprd01.prod.exchangelabs.com, fe80::d6d:5a3d:86f4:b199	mapi id 15.20.3955.018	2021-03-19T16:49:19
2	vi1pr0102mb3167.eurprd01.prod.exchangelabs.com, 2a01:111:e400:7e0a::4e	2a01:111:e400:7e0a::131, db5eur03ft029.mail.protection.outlook.com	microsoft smtp server (version=tls1_2, cipher=tls_ecdhe_rsa_with_aes_256_gcm_sha384) id 15.20.3955.18 via frontend transport	2021-03-19T16:49:19
3	2a01:111:e400:7e0a::50, db5eur03ft029.eop-eur03.prod.protection.outlook.com	db5eur03ht003.eop-eur03.prod.protection.outlook.com, 2a01:111:e400:7e0a::111	microsoft smtp server (version=tls1_2, cipher=tls_ecdhe_rsa_with_aes_256_gcm_sha384) id 15.20.3955.18	2021-03-19T16:49:19
4		2002:a0c:aa16:0:0:0:0:0	smtp id d22csp2828343qvb	2021-03-19T16:49:20

Security headers

arc-authentication-results	i=1; mx.microsoft.com 1; spf=none; dmarc=none; dkim=none; arc=none

X headers

x-ms-exchange-crosstenant-authsource	DB5EUR03FT029.eop-EUR03.prod.protection.outlook.com
x-ms-publictraffictype	Email
x-ms-traffictypediagnostic	DB5EUR03HT003:
x-ms-exchange-messagesentrepresentingtype	1
x-ms-exchange-antispam-messagedata	coLxiKb697ihiuVjyS7RMtiScT++qwxVnmsRNIPsyCYuSh+qKTaQAD4B885tj5j9SZYGhabYnRTI9heOjdoSo8mCRF+u97WPFVaVFfys9h7JgmAqu7Qug1Aal
x-google-smtp-source	ABdhPJw6aSxYvWThdbRKONzsnCvhxRDdEr3hG0x1Okb6JQCf12+SFcsTRCmOGgXzJxsaz1W/04Ve
x-received	by 2002:aa7:cd54:: with SMTP id v20mr10780856edw.80.1616172560336; Fri, 19 Mar 2021 09:49:20 -0700 (PDT)
x-ms-exchange-transport-forked	True
x-microsoft-antispam-message-info	dI7Se/jvrKe/c4F8Uq/X3EN1B075MSvHRj+42WR8WvNFHfV2P+IoY42iQ46DgGfbtdZiMTFekFhgle0QrgtfM4T/j2P0Q+MI4Bdid10Qm1erNio1E6JG2qmF:
x-originatororg	outlook.com
x-ms-has-attach	yes
x-ms-exchange-crosstenant-originalarrivaltime	19 Mar 2021 16:49:19.4742 (UTC)
x-ms-exchange-transport-crosstenantheadersstamped	DB5EUR03HT003
x-microsoft-antispam	BCL:0;
x-tmn	[2GSIXQgTh+J+KVj3hU0l6FWlaLKAjldM]
x-ms-exchange-crosstenant-id	84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa

Phishing Investigation Report - BTLO

x-ms-exchange-crosstenant-rms-persistedconsumerorg	00000000-0000-0000-0000-000000000000
x-ms-exchange-crosstenant-rms-persistedconsumerorg	00000000-0000-0000-0000-000000000000
x-ms-exchange-crosstenant-rms-persistedconsumerorg	00000000-0000-0000-0000-000000000000
x-ms-exchange-crosstenant-rms-persistedconsumerorg	00000000-0000-0000-0000-000000000000
x-eopattributedmessage	0
x-ms-exchange-crosstenant-fromentityheader	Internet
x-incomingheadercount	44
x-ms-office365-filtering-correlation-id	35f7d58b-52ef-46af-b3b5-08d8eaf6f0cd
x-ms-exchange-crosstenant-authas	Anonymous
x-ms-exchange-crosstenant-network-message-id	35f7d58b-52ef-46af-b3b5-08d8eaf6f0cd
x-incomingtopheadermarker	OriginalChecksum:7585B8460280CD3154F452A169E5B30299F6FA4400B34A08781C232163844E2A;UpperCasedChecksum:C08DAFF147292AFCD0C0

Other headers

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:threa EI9l0TxwbFr4hv2QgVU2O8WTvhkUYc0L+nQjR1KqZ5fMdRJeuPyQv/gLmMhZeJICB4gN ejVzNcyO299DSh+yQkH25ELGuYNSv3dkai9I2DpfdO0/+SZjpFnolXANsT/29PIxxlEm
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-SenderADChe b=jkXRplE3flqP0bQwXpfvDjkc0QlGrOLJa+vwtOv6JtGdi0+VFntyrBxgQn1DTQqyx4bLHm71Vl7CZTEV3o3zTHtfZSSKxx0GZ0xURonCmt5UdS/r9+aAhAQDkuDmMp11m72T3
arc-seal	i=2; a=rsa-sha256; t=1616172560; cv=pass; d=google.com; s=arc-20160816; b=kCZr16KOmbcxQ5hzDiTI2ksyThj1usdAC+9D+v2UuV8pOSEsONn8q6I9+0i1AO0krl zkezk4 53D6bgDKWtnn/qASJY8DgMf797MiCwTpt0U0oaxMPQcPfyTddLs2IOM3at073tGZI8nL UQ8A==
arc-seal	i=1; a=rsa-sha256; s=arcselector9901; d=microsoft.com; cv=none; b=VvT4wsAhm1GvyO/RiF8rca1DY0Hroh8G5JdZQOCUNXwxGdGnH7xacufVV1uLYmZ2IqZble+9gepolupL0bFOP9lajUtHeUjMX+FwK7JdlA8jqbpZE3qS4FHna+aKPa2GXnV3
thread-topic	Website contact form submission
delivered-to	johnsmith123@gmail.com
content-type	multipart/mixed; boundary="_004_VI1PR0102MB31679BEF784B62C41CDAEDB282689VI1PR0102MB3167_"
accept-language	en-GB, en-US
thread-index	AQHXG60pM2b+ojN0CkOPbNfmJ2aSpqqLiC32
in-reply-to	<E1IMk2z-00086Y-Jw@se7-syd.hostedmail.net.au>
mime-version	1.0
content-language	en-GB
references	<E1IMk2z-00086Y-Jw@se7-syd.hostedmail.net.au>

Phishing Investigation Report - BTLO

Bodies

#1

Content-Type text/plain

Content

```
_____
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).
```

Extracted emails kinnar1975@yahoo.co.uk, mailer-daemon@se7-syd.hostedmail.net.au

Extracted domains se7-syd.hostedmail.net.au, mx-eu.mail.am0.yahoodns.net, yahoo.co.uk

Extracted IPv4s 188.125.72.73

#2

Content-Type text/html

Content

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<style type="text/css" style="display:none;"> P {margin-top:0;margin-bottom:0;} </style>
</head>
<body dir="ltr">
<div style="font-family: Calibri, Helvetica, sans-serif; font-size: 12pt; color: rgb(0, 0, 0);">
<br>
</div>
<div>
<div id="appendonsend"></div>
<hr tabindex="-1" style="display:inline-block; width:98%">
<div id="divRplyFwdMsg" dir="ltr"><font face="Calibri, sans-serif" color="#000000" style="font-size:11pt"><b>Fro
m:</b> Mail Delivery System &lt;Mailer-Daemon@se7-syd.hostedmail.net.au&gt;<br>
<b>Sent:</b> 18 March 2021 04:14<br>
<b>To:</b> kinnar1975@yahoo.co.uk &lt;kinnar1975@yahoo.co.uk&gt;<br>
<b>Subject:</b> Undeliverable: Website contact form submission</font>
<div> </div>
</div>
<div class="BodyFragment"><font size="2"><span style="font-size:11pt">
<div class="PlainText">This message was created automatically by mail delivery software.<br>
<br>
A message that you sent could not be delivered to one or more of its<br>
recipients. This is a permanent error. The following address(es) failed:<br>
<br>
  kinnar1975@yahoo.co.uk<br>
    host mx-eu.mail.am0.yahoodns.net [188.125.72.73]<br>
    SMTP error from remote mail server after end of data:<br>
    554 30 Sorry, your message to kinnar1975@yahoo.co.uk cannot be delivered. This mailbox is disa
bled (554.30).<br>
</div>
</span></font></div>
</div>
</body>
</html>
```

Extracted emails kinnar1975@yahoo.co.uk, mailer-daemon@se7-syd.hostedmail.net.au

Extracted domains se7-syd.hostedmail.net.au, mx-eu.mail.am0.yahoodns.net, yahoo.co.uk

Phishing Investigation Report - BTLO

#3

Content-Type	text/html
Content	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8"><title>Website contact form submission</title></head><body><style type="text/css">p { margin-bottom: 1em; }</style> First Name: Robertbiolo Last Name: Robertbiolo Email Address: kinnar1975@yahoo.co.uk Mobile: 85471397431 Booking Date: 1977-11-18 Booking Time: RobertbioloXE Services Required: Good earnings from $6500 per day >>>>>>>>>>>>>>> https://35000usdperwwekpodf.blogspot.sg?p=9swghttps://35000usdperwwekpodf.blogspot.co.il?o=0hnd <<<<<<<<<<<<<<< </body></html>
Extracted URLs	https://35000usdperwwekpodf.blogspot.sg?p=9swghttps://35000us...
Extracted emails	kinnar1975@yahoo.co.uk
Extracted domains	35000usdperwwekpodf.blogspot.co.il, 35000usdperwwekpodf.blogspot.sg, www.w3.org, yahoo.co.uk

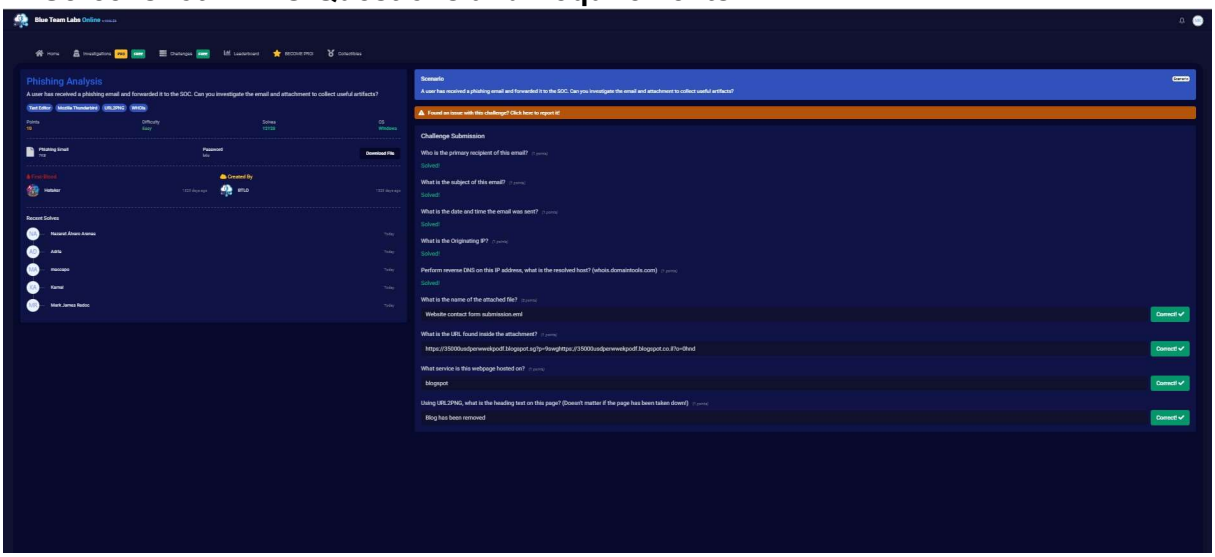
Attachments

#1

Filename	part-000
Size	3.9 Kb
MIME type	RFC 822 mail, ASCII text
SHA256	dff99081b94ba0ffc407411629271f5154ad12555cb5900cfa676e26bf94e04f

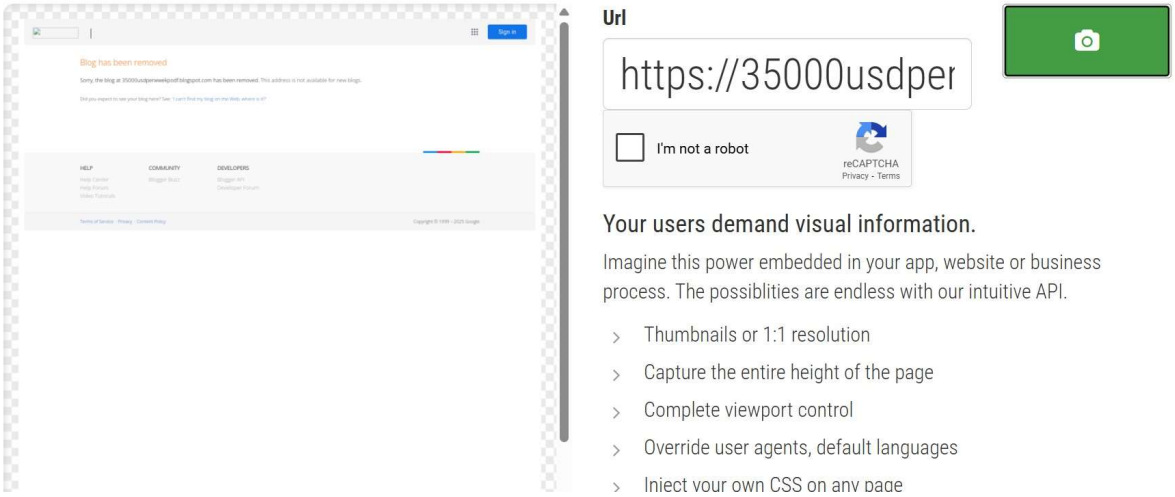
Download

4. Screenshot: BTLO Questions and Requirements



Phishing Investigation Report - BTLO

5. Screenshot: Phishing Website Preview (URL2PNG)



6. Raw Email Content (From Notepad)

Upon reviewing the raw email, the body reveals an HTML form with fake contact form fields and a scam message: 'Good earnings from $6500 per day'. It includes the suspicious embedded link: https://35000usdperwwekpodf.blogspot.sg?p=9swg...

This is a classic phishing lure to trick victims into visiting fraudulent money-making scam sites.

7. Indicators of Compromise (IOCs)

Indicator Type	Value
IP Address	103.9.171.10
Malicious URL	https://35000usdperwwekpodf.blogspot.sg?p=9swg

Recommendations and Mitigation

- Always inspect the full email header before trusting content.
- Use WHOIS and domain reputation tools to verify sender IPs.
- Avoid clicking on unverified shortened or blogspot-style links.
- Implement strong spam filtering across your mail server.
- Report phishing attempts to your internal SOC or IT team.
- Block suspicious IPs (e.g., 103.9.171.10) using system firewalls:
- On Linux: sudo iptables -A INPUT -s 103.9.171.10 -j DROP

Phishing Investigation Report - BTLO

- On Windows: New-NetFirewallRule -DisplayName "Block Malicious IP" -Direction Outbound-RemoteAddress 103.9.171.10 -Action Block

- On Cisco routers: Apply an ACL rule to deny incoming traffic from the IP address.

- On AWS/Azure: Use Network ACL or NSG rules to deny inbound traffic from this IP.