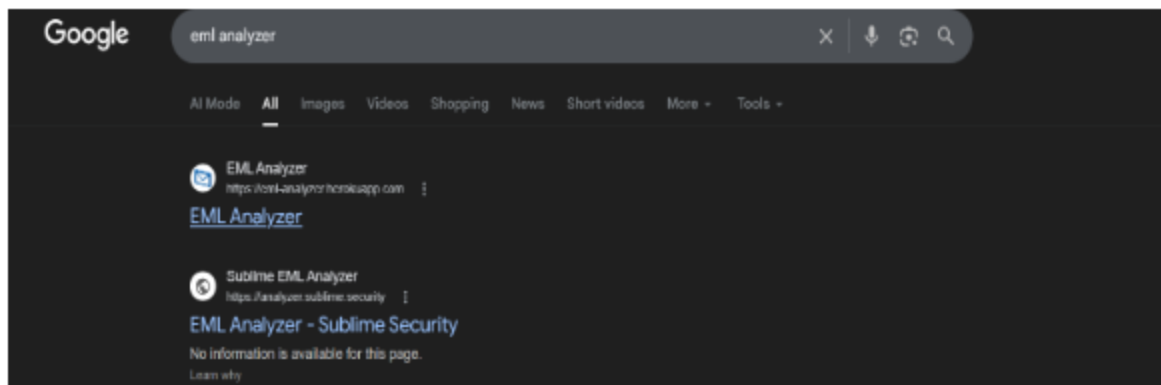



Phishing Email with Malicious Links

```
Received: from mail.nnwifi.com ([173.46.174.49]) by [removed] for
    brad@malware-traffic-analysis.net; Tue, 05 May 2020 13:30:50 +0000 (UTC)
Received: from localhost (localhost [127.0.0.1])
    by mail.nnwifi.com (Postfix) with ESMTTP id 29423C1D28F3
    for <brad@malware-traffic-analysis.net>; Tue, 5 May 2020 08:44:33 -0400 (EDT)
Received: from mail.nnwifi.com ([127.0.0.1])
    by localhost (mail.nnwifi.com [127.0.0.1]) (amavisd-new, port 10032)
    with ESMTTP id jGwPva6p3p_9 for <brad@malware-traffic-analysis.net>;
    Tue, 5 May 2020 08:44:32 -0400 (EDT)
Received: from localhost (localhost [127.0.0.1])
    by mail.nnwifi.com (Postfix) with ESMTTP id 58618C1D3543
    for <brad@malware-traffic-analysis.net>; Tue, 5 May 2020 05:58:55 -0400 (EDT)
Received: from mail.nnwifi.com ([127.0.0.1])
    by localhost (mail.nnwifi.com [127.0.0.1]) (amavisd-new, port 10026)
    with ESMTTP id ACdB6zUvbNRn for <brad@malware-traffic-analysis.net>;
    Tue, 5 May 2020 05:58:55 -0400 (EDT)
Received: from nnwifi.com (94-100-31-27.static.hvvc.us [94.100.31.27])
    by mail.nnwifi.com (Postfix) with ESMTTP id 900EBC20064A
    for <brad@malware-traffic-analysis.net>; Tue, 5 May 2020 03:20:19 -0400 (EDT)
Date: 05 May 2020 07:58:44 -0700
subject: =?UTF-8?B?ICDimqDvuI8gV2FybmluZzogI0KchSBGaw5hbCBub3Rpy2UgOiA=?=malware-traffic-analysis.net=?
From: malware-traffic-analysis.net Support <sues@nnwifi.com>
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html;
    charset="iso-8859-1"
To: brad@malware-traffic-analysis.net

<HTML><HEAD><TITLE></TITLE>
<META name=GENERATOR content="MSHTML 11.00.10570.1001"></HEAD>
<body>
<H2>&nbsp;</H2>
<DIV>&nbsp;</DIV>
```





Drop the EML/MSG file here or click to upload

2020-05-05-phishing-email-example-01.eml

Analyze

Verdicts

oleid

N/A

There is no suspicious OLE file in attachments.

N/A

Headers

Hops

| Hop | From | By | With |
|-----|---|----------------------------|------------------------|
| 1 | 94.100.31.27, nnwifi.com, 94-100-31-27.static.hvvc.us | mail.nnwifi.com | esmtpa id 900ebc20064a |
| 2 | 127.0.0.1, mail.nnwifi.com | 127.0.0.1, mail.nnwifi.com | esmtpt id acdb6zuvbnm |

94.100.31.27

1 / 92

Community Score

1/92 security vendor flagged this IP address as malicious

94.100.31.27 (94.100.28.0/22)
AS 29802 (HVC-AS)

NL

Last Analysis Date
3 days ago

DETECTION

DETAILS

RELATIONS

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

| | | | |
|----------|---------|-------------|-------|
| SOCradar | Malware | Abusix | Clean |
| Acronis | Clean | ADMINUSLabs | Clean |