

Email Analysis

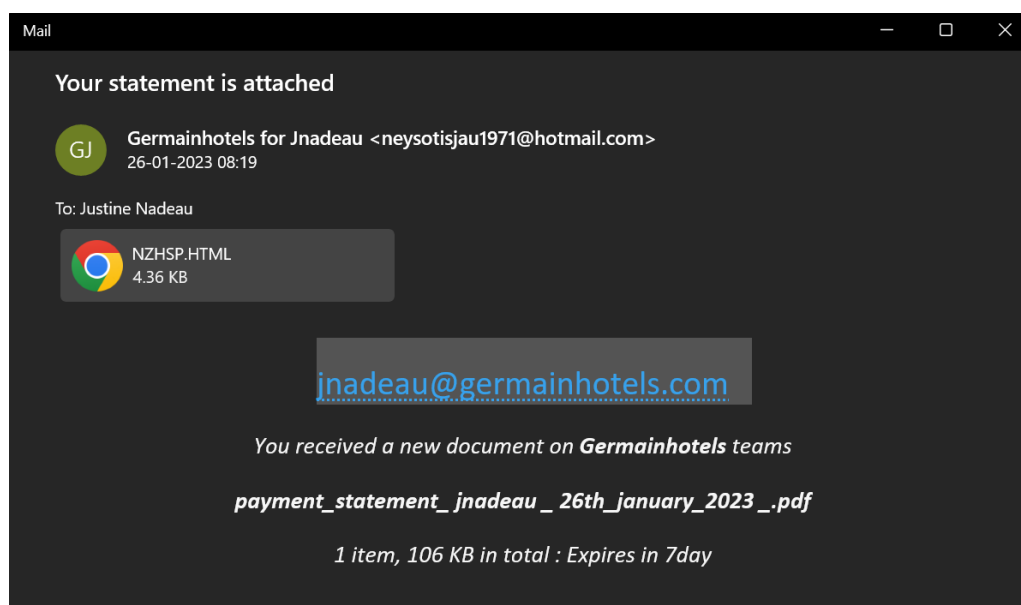
In this example, a malicious email was analysed. The sample was taken from any.run named 'alert_sp2_2.0.0.0 (51).eml'. The email claimed to be from germainhotels and contains the copy of payment statement attached to it. After analysis of the attachment, it was found to be a html file meant for a phishing attempt. After investigation the following artefacts are retrieved:

- Sender: neysotisjau1971@hotmail.com
- Sending Server IP: 40.92.90.99
- Reverse DNS:
mail-vi1eur05olk2099.outbound.protection.outlook.com
- Subject: Your statement is attached
- Attachment Name: NZHSP
- File MD5 Hash: 3E2D964BF08F7FDEAA08C4924DE65DD2

Detailed Analysis Report

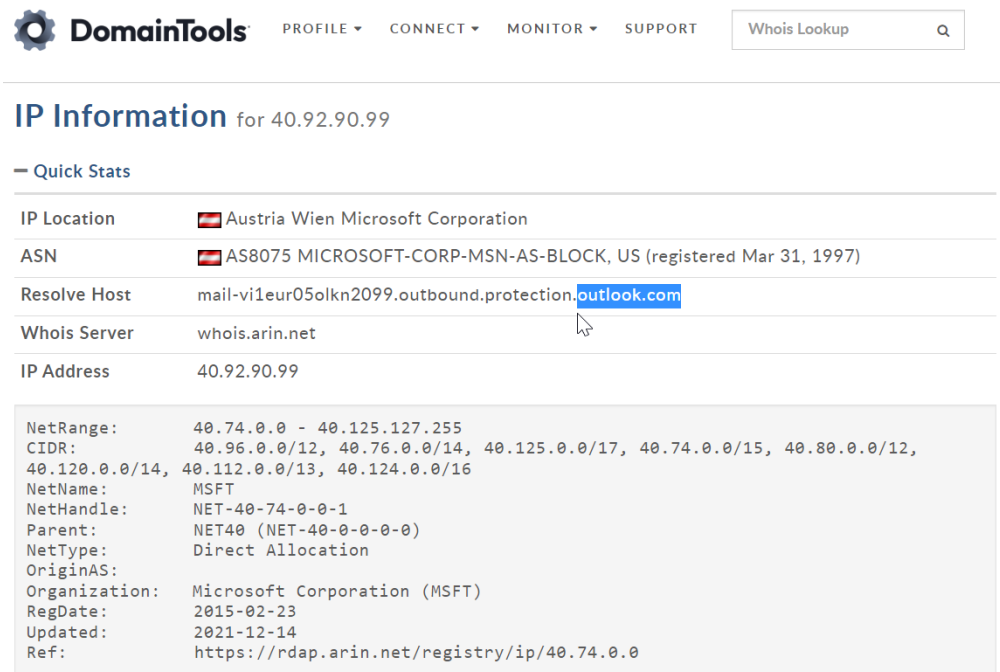
“

[1] The email's formatting raised red flags and didn't appear to originate from the germainhotels.



[2] We are unable to block the sender IP as Outlook is a public domain and blocking it would also block genuine emails.

[3] The specific sender "neysotisjau1971@hotmail.com" can be blocked to stop receiving emails from them in the future.



The screenshot shows the DomainTools website interface. At the top, there's a navigation bar with 'DomainTools' logo and links for PROFILE, CONNECT, MONITOR, and SUPPORT. A search bar labeled 'Whois Lookup' is on the right. Below the navigation bar, the page title is 'IP Information for 40.92.90.99'. Underneath, there's a 'Quick Stats' section with a table of IP details:

IP Location	Austria Wien Microsoft Corporation
ASN	AS8075 MICROSOFT-CORP-MSN-AS-BLOCK, US (registered Mar 31, 1997)
Resolve Host	mail-vi1eur05olk2099.outbound.protection.outlook.com
Whois Server	whois.arin.net
IP Address	40.92.90.99

Below the table, there's a detailed block of information:

NetRange: 40.74.0.0 - 40.125.127.255
CIDR: 40.96.0.0/12, 40.76.0.0/14, 40.125.0.0/17, 40.74.0.0/15, 40.80.0.0/12, 40.120.0.0/14, 40.112.0.0/13, 40.124.0.0/16
NetName: MSFT
NetHandle: NET-40-74-0-0-1
Parent: NET40 (NET-40-0-0-0-0)
NetType: Direct Allocation
OriginAS:
Organization: Microsoft Corporation (MSFT)
RegDate: 2015-02-23
Updated: 2021-12-14
Ref: https://rdap.arin.net/registry/ip/40.74.0.0

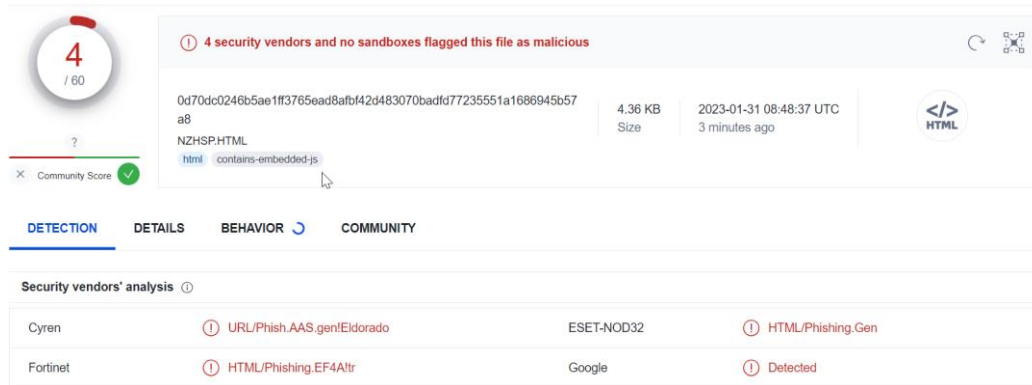
[4] In an effort to generate a sense of urgency, the email also stated that the attached file would expire in seven days, giving the recipient room for error.

[5] Furthermore, A very bad attempt was made to pass off the attached document, 'NZHSP.html', as "payment_statement_jnadeau 26th_January_2023_.pdf".



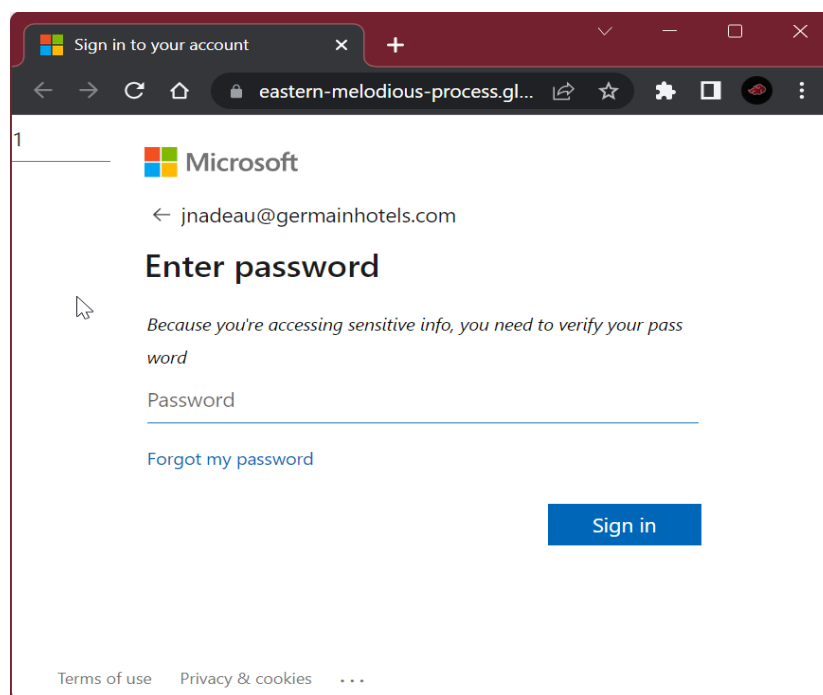
[6] After analysis, it was discovered that the attached file contained embedded_JS and was flagged as phishing by several security vendors on virustotal, including Cyren, Fortinet and Google.

[7] Despite having a low VirusTotal score of 4/60, the file was clearly attempting to harvest credentials.



[8] The phishing page required the recipient's Microsoft password in order to view the file, saying that it was necessary to "check before accessing critical information," but the designed Microsoft login page is a fake and can be identified by paying close attention.

[9] Additionally, the phishing page's address was different from the website for Microsoft accounts.



”