Email Forensics Report – Identification of Forgery and Future Attack Plan

Cyrus Majd

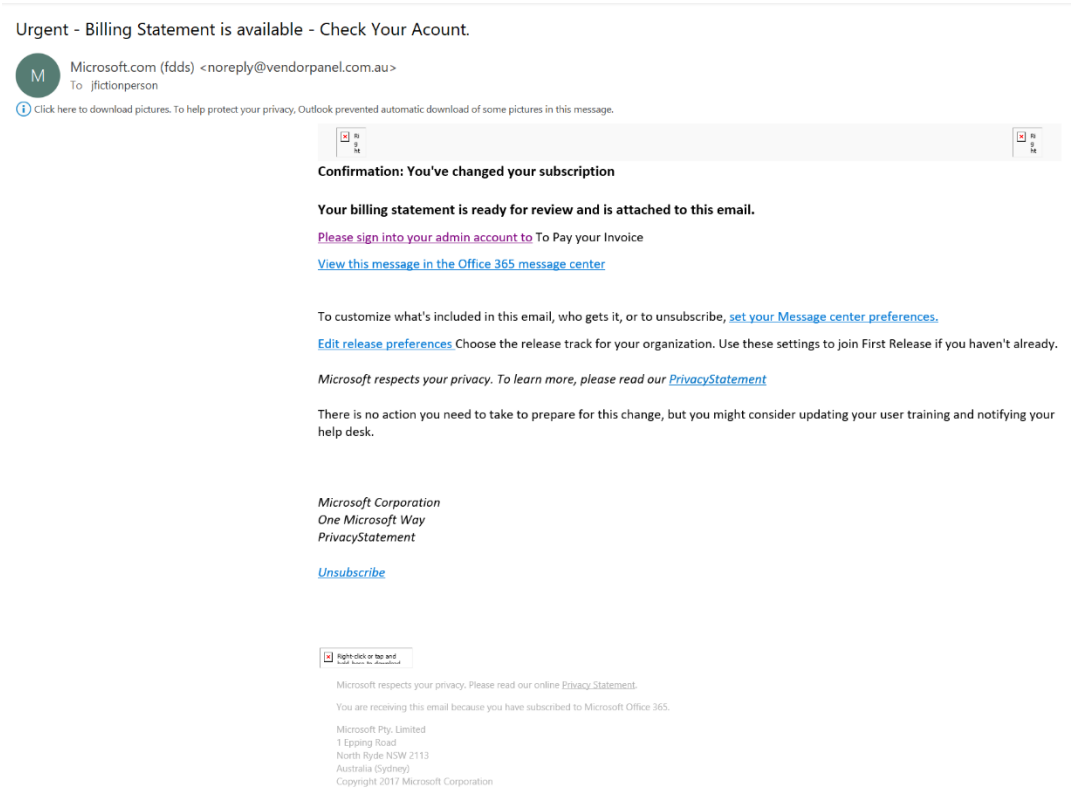
Introduction

We are given an email reported by a user to be a phishing attempt. The task is to identify whether or not the email is truly a phishing attack, and develop a defensive plan to thwart similar attacks in the future.

The approach for identifying this email as a phishing attempt would be to populate a list of *red flags* which will help us better visualize the legitimacy of the email. Depending on the length and contents of the organized list, we can make our decision. It is vitally important to stay completely neutral throughout the investigation, listing only *confirmed* conclusions, as to minimize the effects of confirmation bias in our results.

Analysis

Before we analyze the email headers and delve too deep, we must first investigate the email as it is seen by the actual user.



Urgent - Billing Statement is available - Check Your Acount.

M Microsoft.com (fdds) <noreply@vendorpanel.com.au>
To jfictionperson

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Confirmation: You've changed your subscription

Your billing statement is ready for review and is attached to this email.

Please sign into your admin account to To Pay your Invoice

View this message in the Office 365 message center

To customize what's included in this email, who gets it, or to unsubscribe, set your Message center preferences.

Edit release preferences Choose the release track for your organization. Use these settings to join First Release if you haven't already.

Microsoft respects your privacy. To learn more, please read our PrivacyStatement

There is no action you need to take to prepare for this change, but you might consider updating your user training and notifying your help desk.

Microsoft Corporation
One Microsoft Way
PrivacyStatement

Unsubscribe

Right-click or tap and hold here to download

Microsoft respects your privacy. Please read our online Privacy Statement.

You are receiving this email because you have subscribed to Microsoft Office 365.

Microsoft Pty. Limited
1 Epping Road
North Ryde NSW 2113
Australia (Sydney)
Copyright 2017 Microsoft Corporation

At a glance, we see that the email *seems* to have originated from *vendorpanel.com.au*. The email claims to be from Microsoft however, so let's conduct a quick WHOIS lookup to see if the URL is owned by Microsoft.

```
cyrusthevirus@DESKTOP-A9QR0KQ:~/cProgramming/writtenInVim$ whois vendorpanel.com.au
Domain Name: VENDORPANEL.COM.AU
Registry Domain ID: D407400000001302460-AU
Registrar WHOIS Server: whois.auda.org.au
Registrar URL:
Last Modified: 2019-12-27T19:01:56Z
Registrar Name: Web Address Registration Pty Ltd
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Reseller Name:
Status: serverRenewProhibited https://afilias.com.au/get-au/whois-status-codes#serverRenewProhibited
Registrant Contact ID: R-002263471-SN
Registrant Contact Name: James Leathem
Tech Contact ID: C-001448561-SN
Tech Contact Name: James Leathem
Name Server: NS4-08.AZURE-DNS.INFO
Name Server: NS2-08.AZURE-DNS.NET
Name Server: NS3-08.AZURE-DNS.ORG
Name Server: NS1-08.AZURE-DNS.COM
DNSSEC: unsigned
Registrant: VENDORPANEL PTY LTD
Registrant ID: ACN 129460751
Eligibility Type: Company
```

Right off the bat we can see that this URL is not owned by Microsoft, so this raises suspicion. If we search up `vendorpanel.com.au "Microsoft"` we get a few results all mentioning the same kind of email being sent out from this same sender, all tagged as phishing attempts. This raises a lot of suspicion, but it is still not concrete evidence. We want to find a result detailing `vendorpanel.com.au` as an organization trusted by Microsoft, since such sensitive information like the billing statement the email claims to have should always be received from a trusted source. The email shows "Microsoft.com" as the intended email sender, so we can check for Microsoft.com's SPFs and see if `vendorpanel.com.au` is a trusted sender with a simple `dig` lookup.

```
cyrusthevirus@DESKTOP-A9QR0KQ:~/cProgramming/writtenInVim$ dig @8.8.8.8 -t txt microsoft.com | grep spf1
microsoft.com.          2346    IN      TXT     "v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com include
:_spf-c.microsoft.com include:_spf-ssg-a.microsoft.com include:spf-a.hotmail.com include:_spf1-meo.microsoft.com -all"
```

Unfortunately, `vendorpanel.com.au` is not found in this SPF list, which raises a **red flag**. We will add this to our list.

Now investigating the content of the email, we see that the "`sign in to your admin account`" link actually links:

"`https://nam04.safelinks.protection.outlook.com/?url=`**`http%3A%2F%2Fjonathanmelgoza.com%2FGT%2Findex.php`**`%3Fm%3Djfictionperson%40contosa.com&data=02%7C01%7Cjfictionperson%40contosa.com%7C1718b5657314483fc31508d7bc854d15%7Ccb2bab3d7d9044ea9e31531011b1213d%7C0%7C1%7C637185153025927495&sdata=gJBAM84%2B%2FS35hcJe4KWaAc88BlB7mBIhZCqMsgH%2F4%2B4%3D&reserved=0`"

This "`jonathangoza.com/index.php`" URL certainly doesn't seem to be a website Microsoft should use for logging into a secure admin account. Just to make sure, lets conduct another

WHOIS lookup.

```
cyrusthevirus@DESKTOP-A9QR0KQ:~/cProgramming/writtenInVim$ whois jonathanmelgoza.com
   Domain Name: JONATHANMELGOZA.COM
   Registry Domain ID: 1809553648_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.scip.es
   Registrar URL: http://www.dondominio.com
   Updated Date: 2020-03-04T10:20:40Z
   Creation Date: 2013-06-19T20:36:22Z
   Registry Expiry Date: 2021-06-19T20:36:22Z
   Registrar: Soluciones Corporativas IP, SL
   Registrar IANA ID: 1383
   Registrar Abuse Contact Email: abuse@scip.es
   Registrar Abuse Contact Phone: 34871986387
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NS1721.WEBEMPRESA.EU
   Name Server: NS1722.WEBEMPRESA.EU
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-05-09T04:43:00Z <<<
```

As suspected, the website is privately owned, and shows no affiliation with Microsoft. In fact, it seems that all of the links in the email point to the same `jonathangoza.com/index.php` subpage, with the same php data fields being sent every time. Out of curiosity, I tried to visit the `index.php` subpage so I could try to read and analyze the source code to see what it actually does, but this page does not currently exist. In the meantime, we will add these findings to our list of **red flags**.

This is about all we can find from analyzing the email at face value. To truly determine the email's legitimacy, we need to analyze the email's header in raw form. This will give us lots of more details on the path this email took to get to the user, and any hidden content.

Simply skimming through the email contents at first glance, something suspicious catches our eye: a hunk of text [from lines 181-199] seemingly unrelated to the email received by our client.

```
174   MIME-Version: 1.0
175
176   --------------Boundary-00=_VI2VVA40000000000000
177   Content-Type: Text/Plain; charset=UTF-8
178    Content-Transfer-Encoding: quoted-printable
179
180
181   [IKEA logo]
182   Ol=E1,
183   Obrigado por contactar o Apoio ao Cliente IKEA.
184
185   Recebemos o seu email e responderemos =E0 sua quest=E3o o mais brevemente p=
186   oss=EDvel.
187
188   Este endere=E7o de email n=E3o =E9 monitorizado - n=E3o responda a este ema=
189   il.
190
191   Se precisar de nos contactar, visite a p=E1gina de Contactos em IKEA.pt
192
193   Cumprimentos,
194
195   Apoio ao Cliente IKEA
196
197   As suas informa=E7=F5es s=E3o guardadas de modo a poder dar-lhe o melhor ap=
198   oio poss=EDvel. Encontra aqui a nossa Pol=EDtica de privacidade.<https://ww=
199   w.ikea.com/ms/pt_PT/privacy_policy/privacy_policy.html>
200
```

Putting this through Google Translate, we can roughly make out that this is actually content from an IKEA customer support email. This is a serious **red flag**! If this was really a direct message from Microsoft detailing something as sensitive as a billing statement, it would not have seemingly unrelated content polluting the email and introducing unknown factors and information. We can only speculate where this content came from, but in the meantime we will add it to the red flag list.

Now lets analyze the `Received:` headers, as these are the most reliable sources of information we can extract from the email (these are very difficult to be spoofed or forged). Keep in mind that the topmost `Received:` header is the one closest to the destination, so we need to read the headers from bottom to top in order to map out the email's path. The following is the beginning contents of the earliest `Received:` header.

```
34  Received: from NAM02-CY1-obe.outbound.protection.outlook.com (52.100.132.61)
35  by CO1NAM04FT048.mail.protection.outlook.com (10.152.91.166) with Microsoft
36  SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
37  15.20.2772.15 via Frontend Transport; Fri, 28 Feb 2020 19:35:00 +0000
```

We see that the message at first originated from `51.100.132.61` and was first sent to `10.152.91.166`. A quick WHOIS lookup on both these addresses reveals that the originator is Microsoft (Microsoft owns the 52.96.0.0. – 52.115.255.255 address space) and the first recipient is a privately owned IP address:

```
cyrusthevirus@DESKTOP-A9QR0KQ:~/cProgramming/writtenInVim$ whois 52.100.132.61 | grep NetRange -A10
NetRange:       52.96.0.0 - 52.115.255.255
CIDR:           52.112.0.0/14, 52.96.0.0/12
NetName:        MSFT
NetHandle:      NET-52-96-0-0-1
Parent:         NET52 (NET-52-0-0-0-0)
NetType:        Direct Assignment
OriginAS:
Organization:   Microsoft Corporation (MSFT)
RegDate:        2015-11-24
Updated:        2015-11-24
Ref:            https://rdap.arin.net/registry/ip/52.96.0.0
```

```
cyrusthevirus@DESKTOP-A9QR0KQ:~/cProgramming/writtenInVim$ whois 10.152.91.166 | grep NetRange -A10
NetRange:       10.0.0.0 - 10.255.255.255
CIDR:           10.0.0.0/8
NetName:        PRIVATE-ADDRESS-ABLK-RFC1918-IANA-RESERVED
NetHandle:      NET-10-0-0-0-1
Parent:          ()
NetType:        IANA Special Use
OriginAS:
Organization:   Internet Assigned Numbers Authority (IANA)
RegDate:
Updated:        2013-08-30
Comment:        These addresses are in use by many millions of independently operated networks, which might be as small a
s a single computer connected to a home gateway, and are automatically configured in hundreds of millions of devices.  Th
ey are only intended for use within a private context  and traffic that needs to cross the Internet will need to use a di
fferent, unique address.
```

This indicates that the message *did* in fact originate from Microsoft, but as we further investigate the path the email took, it becomes more evident that it leads to third party proxies which should not be involved in a sensitive Microsoft billing statement. This is another **red flag** and should be noted.

Next, we will look at information just underneath the `Message-ID:` field and before the beginning of the `X-` fields. Below is a screenshot.

```
From: Microsoft.com (fdds) <noreply@vendorpanel.com.au>
To: "jfictionperson" <jfictionperson@contosa.com>
Subject: Urgent - Billing Statement is available - Check Your Acount.
Return-Path: IINmQNpUdyQT@ramars.com
Reply-To: "Microsoft" <aqmith@aol.com>
Date: Fri, 28 Feb 2020 19:34:56 +0000
```

Immediately, we notice a few strange things. Firstly, the `From:` field and `Return-Path:` fields do not match. The from address *can* be set to any arbitrary value, but we often see mismatches between these fields in *forged messages*. In addition to this, the Return-Path leads to a strange email address at *ramars.com*, which is a small architecture company. An important Microsoft email should not even mention such an unrelated domain, much less include it as a Return-Path. This is a **red flag** worthy of note.

We also see that the `Reply-To:` field actually points to a privately owned email address, masquerading as "Microsoft". This is another serious **red flag**, as it is an indication that some tricky spoofing is at play here.

Now lets investigate some of the `X-` header fields. A particular field catches our eye, which seems to reveal an originator IP address:

```
129   X-MS-Exchange-CrossTenant-OriginalAttributedTenantConnectingIp: TenantId=dfe85f9d-4cf5-42ca-af2b-cb428f5d0d2f;Ip=[
      88.198.196.162];Helo=[ramars.com]
```

`X-` headers are extensions of normal RFC headers. They can contain extra information on the contents of the email. An important header to look for is often similar to "X-Originating-IP", because it can sometimes store the IP address of the machine sending the message. In our email, we find that the originating IP is 88.198.196.162. A quick WHOIS lookup reveals that this IP is owned by a private company "HETZNER".

```
cyrusthevirus@DESKTOP-A9QR0KQ:~/cProgramming/writtenInVim$ whois 88.198.196.162
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '88.198.196.160 - 88.198.196.175'

% Abuse contact for '88.198.196.160 - 88.198.196.175' is 'abuse@hetzner.de'

inetnum:        88.198.196.160 - 88.198.196.175
netname:        HETZNER-fsn1-dc7
descr:          Hetzner Online GmbH
descr:          Datacenter fsn1-dc7
country:        DE
```

We don't know much about HETZER, and we don't need to. A real Microsoft email should have nothing to do with such an unrelated company. This is another **red flag**.

Lets go back to our normal header fields. On lines 60-61 and lines 32-33, we find a `Received-SPF` field.

```
32    Received-SPF: None (protection.outlook.com: ramars.com does not designate
33     permitted sender hosts)
```

This is interesting. It seems that we may have failed SPF, and that *ramars.com*¸ another unrelated website we find in the email, is not registered by Microsoft to send out emails on their behalf. We can verify this with the same `dig` command we used on page 1.

```
cyrusthevirus@DESKTOP-A9QR0KQ:~/cProgramming/writtenInVim$ dig @8.8.8.8 -t txt microsoft.com | grep spf1
microsoft.com.          2346    IN      TXT     "v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com include
:_spf-c.microsoft.com include:_spf-ssg-a.microsoft.com include:spf-a.hotmail.com include:_spf1-meo.microsoft.com -all"
```

Sure enough, ramars.com is not a part of this list. This is another major **red flag.**

At this point, we have manually searched through the email headers and have found lots of red flags to report, but we should also verify our findings with some sort of tool to minimize any human error. There are many email header analyzer tools online. I decided to first use https://toolbox.googleapps.com/apps/messageheader/analyzeheader. Most of our findings agree to the online analyzer's conclusions, but one critically important new piece of information pops out at us – the DMARC authentication failed.

DMARC: **fail**

This is serious news, because DMARC is a protocol for authenticating than an email sent from an organization's domain is a legitimate message and not forged. For DMARC to fail, both SPF and DKIM protocols have to fail as well. DMARC can help prevent direct-domain spoofing, so if it has failed, this protection is removed from the email as well. To make sure of this finding, I used another tool, https://mxtoolbox.com/EmailHeaders.aspx, to cross-check my results. Sure enough, the results show the same conclusions:

- DMARC Compliant
  - SPF Alignment
  - SPF Authenticated
  - DKIM Alignment
  - DKIM Authenticated

This is possibly our **biggest red flag** that this email has been forged.

Results

The forensic investigation delivers an extensive list of red flags which lead on the conclusion that **the email in question was, in fact, a phishing attack.** The list of red flags are given below for reference:

List of Red Flags:

1) **Email sender [VENDORPANEL.COM.AU] is not a trusted party of Microsoft (intended sender)**

2) **Links in the email lead to URL [jonathangoza.com/index.php], with multiple populated parameter fields. A true Microsoft billing alert should not link to a privately owned site with no affiliation with Microsoft.**
3) **Extra, unrelated content from an IKEA customer support email found in our client's received email.**
4) **Traffic passes through private email servers.**
5) **Envelope Sender Address (Return-Path) field mismatch with From: field, and Return-Path leads to suspicious-looking user at a company unrelated to Microsoft or any of its services.**
6) **Reply-To: field spoofs Microsoft but instead points to privately owned .aol email address**
7) **"X-Origin-IP" X- header points to another domain unrelated to Microsoft.**
8) **"ramars.com" Received-SPF check: the domain is not a permitted sender host for Microsoft.**
9) **DMARC authentication failure, DKIM authentication failure, SPF authentication failure.**

Future Attack Mitigation Plan

Phishing attacks pose a great risk to any individual or organization. Below is a list, in order of priority, (1 = highest priority) of approaches/steps to mitigate such attacks in the future.

1. Make sure the company email provider uses DMARC and **strictly only allows messages where DMARC is authenticated**. DMARC is the only email authentication protocol that ensures spoofed emails do not reach potential victims.
2. Have employees always check the **email's originating email address**, along with the contents of **any and all hyperlinks** in the email, to make sure they don't redirect to another phishing or data mining site. This is important because if an employee is not careful and does not pay attention to these illegitimate addresses, they can reveal critical information to an attacker. Also teach employees to always run attachments through antivirus software, and to download them *only if* they are confident that it came from a trustworthy source. This step is **incredibly important**, because phishing fundamentally relies on human error. By reducing human error through better educated employees, the risk of phishing attacks is dramatically lowered.
3. Teach staff that technically *everything* within an email message **can be forged** or otherwise tampered with, and the only headers you can truly trust are those by MTAs (mail transfer agents) you trust, such as those under your administrative control.
4. Make sure all digital infrastructure is constantly up to date. This includes **spam filters/detectors** in email clients, and also **antivirus software** on company computers, in the scenario that an employee does fall for the bait and accidentally installs a malicious program.
5. Reduce user privileges for company employees so that they do not accidentally install malicious programs.

6. Enforce dual factor authentication, so that even if an attack does occur and some credentials are lost, the phisher still does not have enough information to fully compromise infrastructure.
7. Make sure all employees have different passwords for different accounts. This way, if they do succumb to a phishing attack, not all of the company's data is compromised.

All in all, the best way to thwart future phishing attacks is to keep company security infrastructure updated and well maintained and to educate/train employees on what phishing attacks look like and how they work. This eliminates most of both the technical and human-error contributors to successful attacks, which dramatically decreases the likelihood of a successful attack.