
Account Takeover Alerts

<https://campus.barracuda.com/doc/84967549/>

Impersonation Protection alerts the administrator when it detects an account takeover [via email](#) and from [within Barracuda Account Takeover](#).

For details on handling an account takeover alert, refer to [Handling an Account Takeover](#).

Alert Frequency

An alert is sent as soon as a user account is determined to be compromised. To prevent inundating the system with alerts, only one alert is sent per day for the same compromised user account. If you take steps to secure this user account so it is no longer compromised, additional alerts will not be sent. As long as the user account remains compromised, Impersonation Protection will continue to send a maximum of one alert per day.

Viewing Alerts

To view alerts:

- From the **Spear Phishing Protection** page, in the **Account Takeover Protection** section, click **View Account Takeover Alerts**.
- Alternatively, click the menu button in the top left corner and select **Account Takeover Protection**. The **Alerts** tab displays.

The **Alerts** table keeps a record of alerts created for your account. Alerts are labeled as follows:

- **Not reviewed** – You have not addressed the alert.
- **Reviewed** – You clicked **Create Incident** for this alert. It is marked as **Reviewed** regardless of whether you completed the incident creation.
- **False Positive** – You determined the activity was legitimate and reported it as a false positive.

26 outstanding alerts (in the last 30 days)

856 incidents created

Apr 02, 2020 5:38 PM latest alert

[NEW INCIDENT](#)

ALERTS
INCIDENTS
INBOX RULES
SIGN INS

ALERTS
Account takeover incidents detected by Sentinel's AI

[EXPORT TO CSV](#)

Date	Account taken over	Activity	Status	
Apr 03, 2020	neil@sookasa.onmicrosoft.com neil@sookasa.onmicrosoft.com	Suspicious email sent from account Suspicious inbox rule added to account	Not reviewed	REVIEW
Apr 02, 2020	Aseem aseem@sookasa.onmicrosoft.com	Suspicious inbox rule added to account	Not reviewed	REVIEW
Apr 01, 2020	Lior Gavish lior@sookasa.onmicrosoft.com	Suspicious email sent from account Suspicious inbox rule added to account	Reviewed	
Mar 30, 2020	Aseem aseem@sookasa.onmicrosoft.com	Suspicious inbox rule added to account	Not reviewed	REVIEW
Mar 29, 2020	Neil Shah neil@sookasa.onmicrosoft.com	Suspicious email sent from account Suspicious sign in Suspicious inbox rule added to account	Not reviewed	REVIEW
Mar 28, 2020	Kelly Chang kpchang@sookasa.onmicrosoft.com	Suspicious sign in	Not reviewed	REVIEW
Mar 27, 2020	Grant Ho grant@sookasa.onmicrosoft.com	Suspicious email sent from account Suspicious inbox rule added to account	Not reviewed	REVIEW
Mar 26, 2020	asaf@sookasa.onmicrosoft.com asaf@sookasa.onmicrosoft.com	Suspicious email sent from account	Reviewed	
Mar 25, 2020	Grant Ho grant@sookasa.onmicrosoft.com	Suspicious email sent from account Suspicious sign in	Reviewed	
Mar 24, 2020	lior@sookasa.onmicrosoft.com lior@sookasa.onmicrosoft.com	Suspicious email sent from account Suspicious inbox rule added to account	Reviewed	

Page: 1 1 - 10 of 135 < >

Reviewing Details

To review details, click **Review** or click the clipboard icon . Available information displays on the three tabs: **Emails Sent**, **Sign Ins**, and **Inbox Rules**. In the example below, you can see there are zero emails sent, five sign ins, and no inbox rules.

Suspicious activity on ctadiparth@barrick.com

EMAILS SENT (0)

SIGN INS (5)

INBOX RULES (0)

VIEW RELATED SIGN INS

Date	IP	User agent	Location	Issue
Oct 14, 2019 9:32 AM	103.236.193.130	Windows/10 - Chrome	India	Unusual location and application
Oct 14, 2019 9:32 AM	103.236.193.130	Windows/10 - Chrome	India	Unusual location and application
Oct 14, 2019 9:32 AM	103.236.193.130	Windows/10 - Chrome	India	Unusual location and application
Oct 14, 2019 9:32 AM	103.236.193.130	Windows/10 - Chrome	India	Unusual location and application
Oct 14, 2019 9:31 AM	103.236.193.130	Windows/10 - Chrome	India	Unusual location and application

Page: 1

1 - 5 of 5

<

>

MARK AS FALSE POSITIVE

CREATE INCIDENT

From here, you can view details of the emails sent.

Create an Incident

If you determine that an account has been compromised, you can create an incident right from the alert. Click **Create Incident**. Follow the instructions in [Handling an Account Takeover](#).

Note that if you create an incident from an alert, the incident might be based on an inbox rule or suspicious sign in. In these cases, you know which of your accounts was compromised, but you might not have a suspicious email. When you are working with the wizard, you can specify that you do not have a sample of a malicious email.

Incidents display on the **Incidents** tab.

Report False Positive

If Impersonation Protection detected suspicious activity, but you are certain the activity was legitimate, click **Report False Positive**.

For more information on false positives and reporting false positives from other locations, refer to [False Positives](#).

Sign Ins Tab Information

On the **Sign Ins** tab, you can see the date, IP, user agent, location, and issues of suspicious sign ins. Click **View Related Sign Ins** to view legitimate sign ins in addition to the suspicious sign ins.

Note that this data is stored for 30 days, so if an alert is more than 30 days old, it is not possible to show all sign ins.

In this view, highlighted rows show events that triggered an Account Takeover alert.

Alert Email Messages

Alert messages can be sent to the administrator with information about the event including the potential target of the account takeover, details of the event, and reasons account takeover is suspected.

ACTION NEEDED

Account takeover detected

Possible account takeover detected for:

[s@.au](#)

[LOG IN TO REVIEW](#)

Why am I getting this alert?

A sign in to the above account was determined by the AI to be suspicious. See details below.

Sign in details

User: S <s@.au>

IP: 120.22.163.180

User agent: Windows/None - Other

Location: Australia

Date/Time: 2023-04-18 - 03:53:25

Analysis

- This sign in comes from an unusual location (Australia)
- This sign in uses an unusual application (Windows/None - Other)

The **Date/Time** of the event is in UTC (Coordinated Universal Time). Your browser's configured time (likely your local time) is used when viewing from within Barracuda Impersonation Protection.

Figures

1. alertsList.png
2. clipboard.png
3. ATOalert.png
4. ato-alert.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.