

## Account Takeover Attacks and their Signals

<https://campus.barracuda.com/doc/89096736/>

In Account Takeover (ATO) / Account Compromise attacks, the attacker uses compromised credentials to take over a targeted account, potentially:

- signing into the account
- sending emails from the account
- altering inbox rules for the account

Inbox rules are only monitored for accounts with paid licenses. Free or student mailbox rules are not monitored.

The compromised credentials can come from password data breaches or from other phishing attacks.

This article provides a general sense of the signals used by Impersonation Protection to detect account takeover attacks. Note that it would be irresponsible to disclose the inner workings of Impersonation Protection.

Impersonation Protection also detects signals to protect you from targeted phishing attacks. See [Targeted Attacks and their Signals](#) for details.

### Emails Sent

The attacker might send impersonated emails to:

- Compromise more credentials
- Distribute malware beyond the gateway
- Commit wire fraud and other social engineering attacks

Suspicious activity on **lior@sookasa.onmicrosoft.com**

EMAILS SENT (5)   SIGN INS (0)   INBOX RULES (1)

Date	Recipient	Subject	
Oct 29, 2018 1:33 PM	Shane Barry and 1 other recipient shane@sookasa.onmicrosoft.com	Please DocuSign these documents: Offer Holt-Anderson.pdf	<a href="#">VIEW MESSAGE</a>
Oct 29, 2018 1:32 PM	Asaf Cidon and 1 other recipient asaf@sookasa.onmicrosoft.com	Please DocuSign these documents: Offer Holt-Anderson.pdf	<a href="#">VIEW MESSAGE</a>
Oct 29, 2018 1:32 PM	Alexey Tsitkin and 1 other recipient alexey@sookasa.onmicrosoft.com	Please DocuSign these documents: Offer Holt-Anderson.pdf	<a href="#">VIEW MESSAGE</a>
Oct 29, 2018 1:31 PM	Itay Bleier and 1 other recipient itay@sookasa.onmicrosoft.com	Please DocuSign these documents: Offer Holt-Anderson.pdf	<a href="#">VIEW MESSAGE</a>
Oct 29, 2018 1:31 PM	Nadia Korshun and 1 other recipient nadia@sookasa.onmicrosoft.com	Please DocuSign these documents: Offer Holt-Anderson.pdf	<a href="#">VIEW MESSAGE</a>

Page: 1 1 - 5 of 5 < >

[CLOSE](#)

For more information, see [Account Takeover Alerts](#) and [Handling an Account Takeover](#).

## Suspicious Sign Ins

The attacker might sign into an account to send emails, change policies, or perform other tasks while logged in as a valid user.

Suspicious activity on **itay@sookasa.onmicrosoft.com**

EMAILS SENT (0)   **SIGN INS (1)**   INBOX RULES (0)

[VIEW RELATED SIGN INS](#)

Date	IP	User agent	Location	Issue
Jul 03, 2019 8:46 AM	45.64.176.254	CBAInProd	Nigeria	Unusual location and application

Page: 1 1 - 1 of 1 < >

[CLOSE](#)

For more information, see [Suspicious Sign Ins](#).

## Inbox Rules

The attacker might change rules to cover their tracks, for example creating rules to route certain incoming emails to their own, separate account.

Suspicious activity on **itay@sookasa.onmicrosoft.com**

EMAILS SENT (0)

SIGN INS (0)

INBOX RULES (1)

Date	Sequence	Name	Actions	Conditions	Exceptions	Enabled
Jul 02, 2019 6:40 AM	1	Critical security alert for your account	Stop processing rules Delete message		No	Yes

Page: 1 1 - 1 of 1 < >

CLOSE

For more information, see [Investigating Inbox Rules](#).

## Figures

1. emailSent.png
2. signIns.png
3. inboxRules.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.