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.

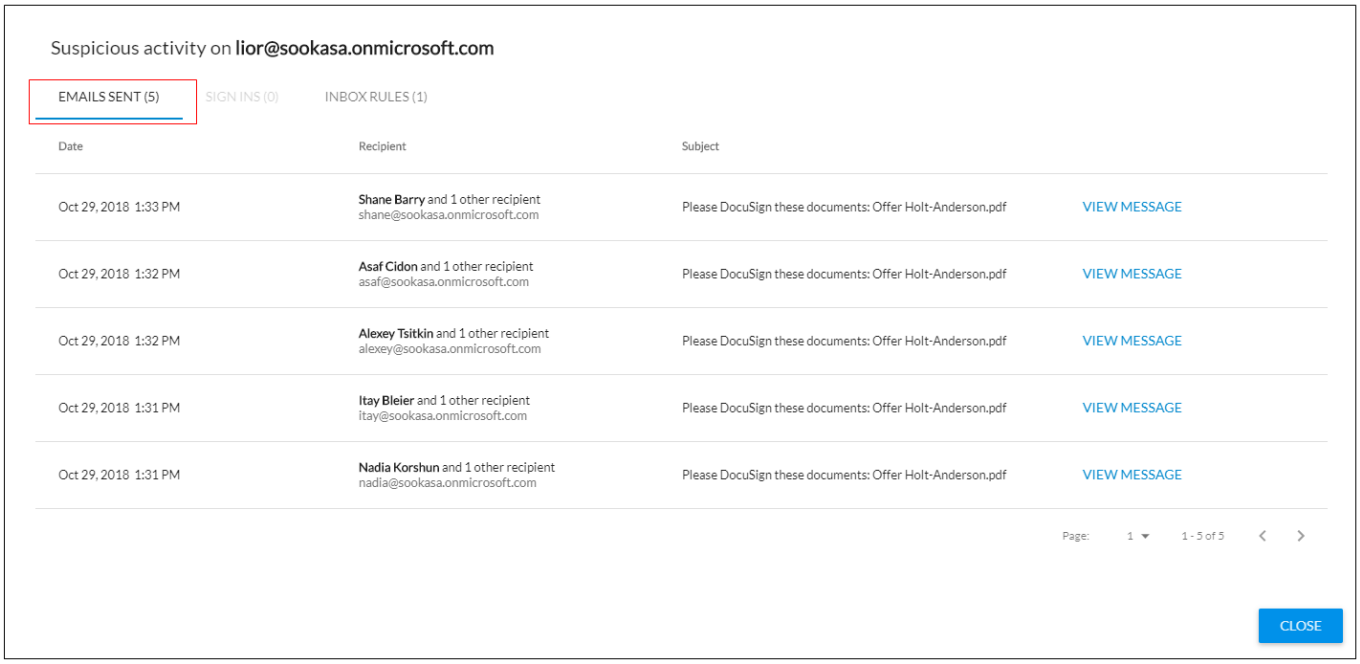
This article provides a general sense of the signals used by Impersonation Protection to detect account takeover attacks. Note that it would be irresponsible to disclose the inner workings of Impersonation Protection.

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:

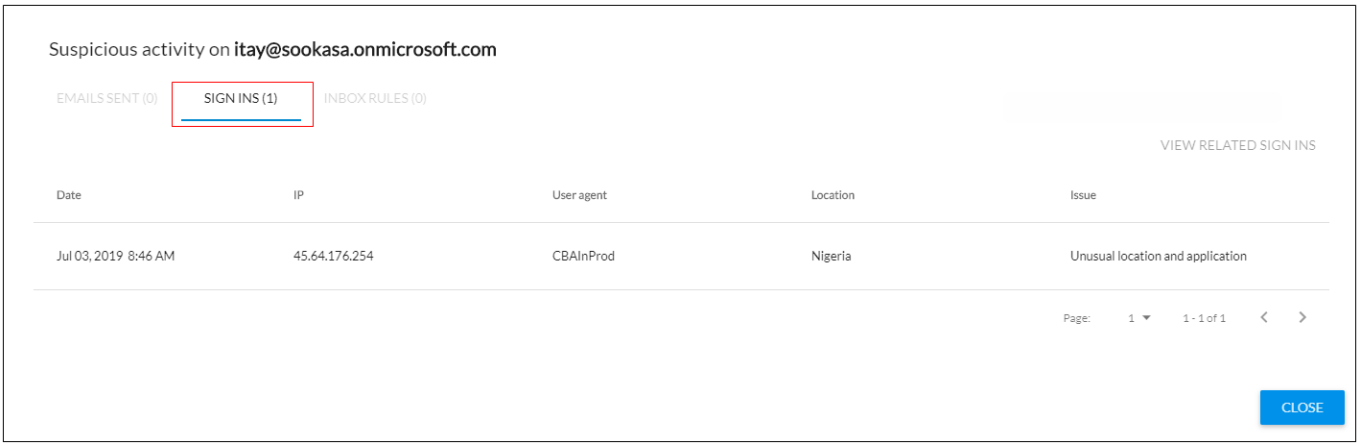
- Compromise more credentials
- Distribute malware beyond the gateway
- Commit wire fraud and other social engineering attacks



For more information, see Account Takeover Alerts and Handling an Account Takeover.

Suspicious Sign Ins

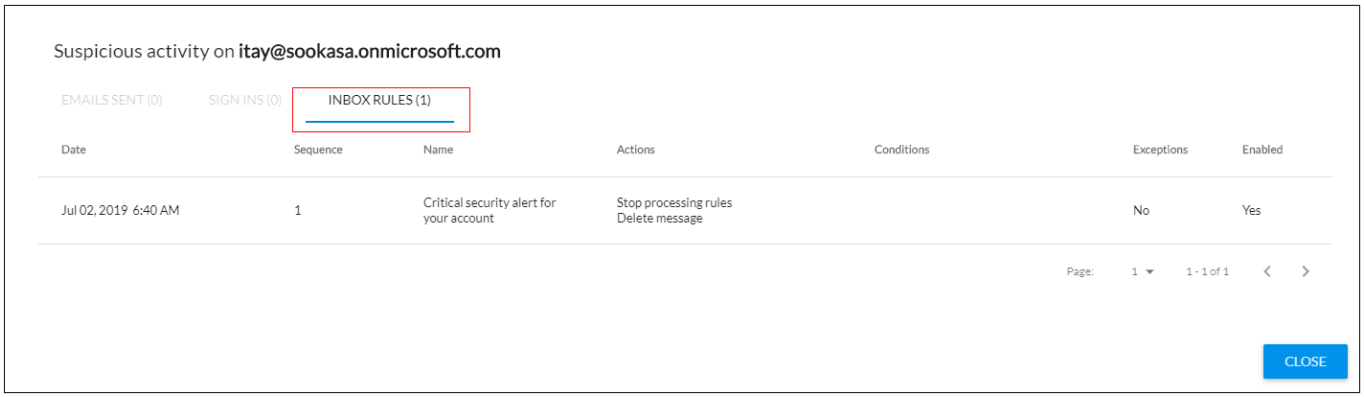
The attacker might sign into an account to send emails, change policies, or perform other tasks while logged in as a valid user.



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.



For more information, see Investigating Inbox Rules.

Figures

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