SaaS Alerts™

# Session Token Hijacking and Business Email Compromise

## How to spot it and beat it

We're all familiar with brute-force attacks. They've been the backbone of hackers' strategies for years. However, we're increasingly seeing a different kind of attack: token hijacking. This new method of attack raises concerns since it allows hackers to bypass multifactor authentication (MFA) and Conditional Access.

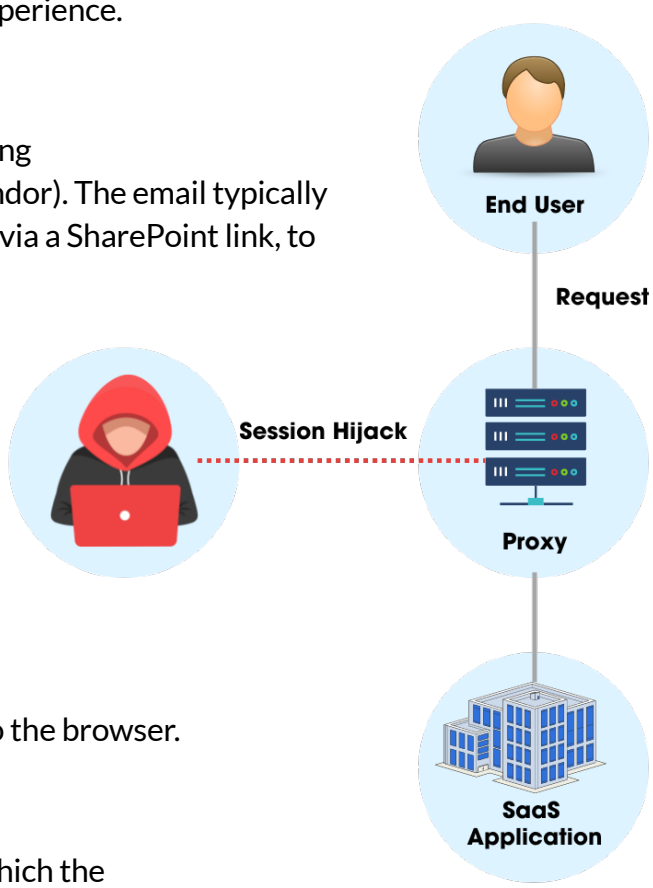
## Token hijacking in FIVE simple steps

### Step 1

A bad actor sets up a server between the end-user's login screen and the Software-as-a-Service (SaaS) service being logged into (Microsoft 365, for example). The server mimics the tool's exact login experience.

### Step 2

The hacker then sends an email (usually impersonating someone that the end user knows, like a client or vendor). The email typically includes a login link to the SaaS application, perhaps via a SharePoint link, to download a document.




### Step 3

The end user clicks on the link. And why wouldn't they? The email and link both look like something they click on every day of the week.

### Step 4

The end user is prompted to enter their credentials. When they do, an access token is created and sent to the browser.

### Step 5

The token is intercepted by the bad actor's server, which the attacker can now use to access the end-user's account.

## How to spot token hijacking

Token hijacking is essentially a business email compromise (BEC) event. In order to identify BEC in its early stages (i.e., prior to any loss), there must be continuous observation of account behavior and recognition of activity that:

- Does not fit the typical pattern of account usage
- Takes "classic" actions that indicate BEC, such as:
  - Setting up email forwarding rules
  - Forwarding to an external address
  - Redirecting internal folders
  - Modifying MFA methods
  - Adding SMS, new phone
  - Adding new authenticator apps
  - Modifying account administrator roles
  - Accessing accounts from new, often unusual locations
  - Accessing accounts from new device(s)

Any of these activities taken individually may seem harmless, but they should still be monitored and logged. When observed together in a relatively short time sequence, these activities create an indicator of compromise (IOC).

## How to prevent it

Token hijacking bypasses MFA and Conditional Access. The only way to beat this new threat vector is good anti-phishing education AND continuous monitoring of account behavior to block account access when behavior anomalies are detected.