SaaS Alerts
A Kaseya COMPANY

DATA SHEET

Session Token Hijacking & 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. But we're increasingly seeing a different kind of attack: token hijacking. This new method of attack raises concern because it allows hackers to bypass MFA and Conditional Access.

TOKEN HIJACKING IN 5 SIMPLE STEPS

STEP 1

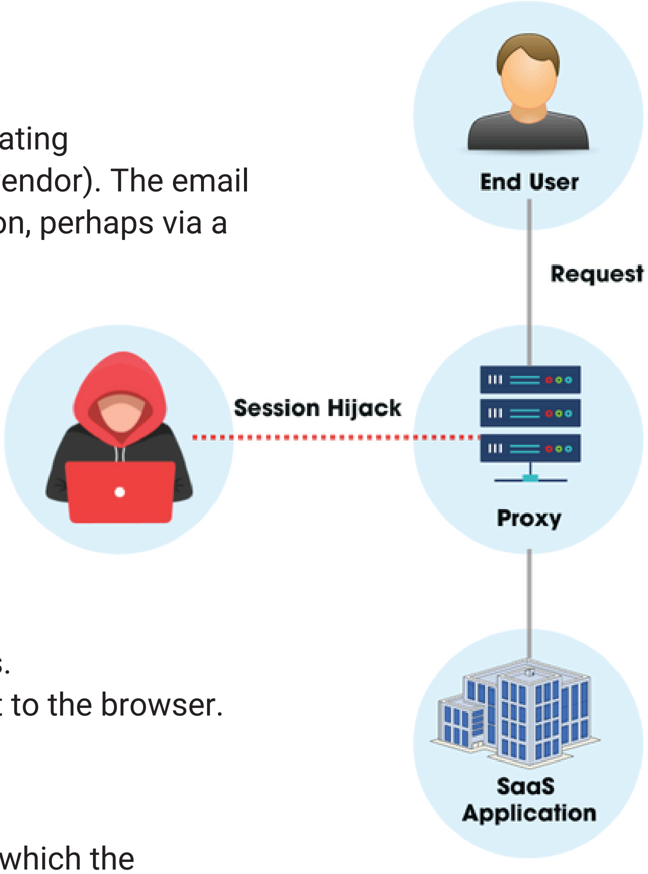
A bad actor sets up a server between the end-user's login screen and the SaaS service being logged into (Microsoft 365, for example). The server mimics the tool's exact login experience.

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:
  - Setup email forwarding rules
  - External address forwarding
  - Internal folder redirection
  - Modify MFA methods
  - Add SMS, new phone
  - Add new authenticator app
  - Modify account administrator roles
  - Access account from new, often unusual locations
  - Access account from new device(s)

Any of these activities taken individually can be innocent enough, 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.

SaaS Alerts
A Kaseya COMPANY

For more information, contact us at
sales@saasalerts.com
or visit
www.saasalerts.com