INCIDENT REPORT

Device code phishing — token replay against r.veldman@domain.nl

True Positive · 90%

AT A GLANCE

Tenant	Demo Customer (domain.nl)
Microsoft incident	#4471
Severity	High
Classification	True Positive
Pipeline status	completed
Analyzed by	IVON (auto)
Opened	2026-05-26 13:14 UTC
Completed	2026-05-26 13:24 UTC

WHAT MICROSOFT DETECTED

Microsoft classified this incident as **TruePositive** (determination: **Compromised account**).

ALERT	SOURCE	SEVERITY	MITRE
Anomalous device code sign-in with unfamiliar user agent	Microsoft Entra ID Protection	High	`T1566` `T1078.004`
Sign-in from an atypical location for the user	Microsoft Entra ID Protection	Medium	`T1078`
Token replay blocked by Conditional Access (AADSTS53003)	Microsoft Sentinel	Medium	`T1550.001`

EXECUTIVE SUMMARY

> Confirmed device code phishing against **r.veldman@domain.nl**. The user completed an attacker-initiated device code flow on 20 May 2026 and tokens were issued — the phish succeeded at the authentication step. Exploitation was stopped only because the attacker's token replay came from a German IP (`91.64.122.203`, `python-requests/2.33.1`) and hit a location-based Conditional Access block (**AADSTS53003**). No mailbox access, inbox/forwarding rules, OAuth grants or device registration were observed — but that is a consequence of the replay being blocked, not of the flow being caught upstream. Treated as a true positive.

What the initial alert flagged: An anomalous device code sign-in for r.veldman@domain.nl with an unusual user agent, raised against the Sentinel workspace for domain.nl. The reporting analyst suspected an EvilTokens-style device code phish leading to attacker device registration.

METHODOLOGY

- All sign-ins for the user over 30 days, broken down by authentication protocol, app and result.
- The two successful `deviceCode` authentications on 20 May (10:24 UTC) and the browser-leg IPs Entra evaluated for Conditional Access.
- Device-related `AuditLogs` operations for the user, to confirm or rule out attacker device registration.
- Non-interactive sign-ins and token replay from the IPs involved.
- Lateral spread: whether the attacker IPs touched any other user in the tenant.

FINDINGS

- The device code flow completed successfully from NL IPs `77.62.148.19` and `94.157.203.44` — tokens were issued (post-consent was reached).
- Both IPs were only ever seen with "Microsoft Authentication Broker", never with normal applications — consistent with a device code broker leg rather than legitimate use.
- A token replay was attempted from `91.64.122.203` (Germany) using `python-requests/2.33.1` — a classic EvilTokens automation fingerprint.
- Both replay attempts returned **AADSTS53003** (Conditional Access block, location / named-locations based). Exploitation was blocked at replay, not at the phish.
- No mailbox access, inbox or forwarding rules, OAuth grants, or device registrations were observed — a consequence of the replay being blocked, not of the flow being caught upstream.
- A password reset fired at 10:26:03, inside the attack window — provenance unverified (user, admin response, or a token-derived SSPR path).

RECOMMENDATION

Suggested remediations (pending customer approval):

- `revoke_user_sessions` → user:r.veldman@domain.nl
- `require_password_reset` → user:r.veldman@domain.nl
- `audit_auth_methods` → user:r.veldman@domain.nl
- `block_device_code_flow` → ca_policy:tenant-wide

TIMELINE & TACTICS

Indicators of compromise:

- ip: 91.64.122.203 (token replay, Germany)
- ip: 77.62.148.19 (device code browser leg, NL)
- ip: 94.157.203.44 (device code browser leg, NL)
- user_agent: python-requests/2.33.1
- account: r.veldman@domain.nl
- tooling: EvilTokens device-code phishing

Timeline

TIMESTAMP (UTC)	ACTION	ACTOR	IP	NOTES
2026-05-20T10:24:11Z		r.veldman@domain.nl	77.62.148.19	Anomalous

TIMESTAMP (UTC)	ACTION	ACTOR	IP	NOTES
	Device code authentication succeeded (tokens issued)			
2026-05-20T10:24:58Z	Second device code authentication (Authentication Broker)	r.veldman@domain.nl	94.157.203.44	Anomalous
2026-05-20T10:25:40Z	Token replay attempt via python-requests/2.33.1	attacker	91.64.122.203	Anomalous
2026-05-20T10:25:42Z	Conditional Access blocked the replay (AADSTS53003)	attacker	91.64.122.203	Anomalous
2026-05-20T10:26:03Z	Password reset (provenance unverified)	r.veldman@domain.nl	—	Anomalous

MITRE tactics: `Phishing (T1566)` `Steal Application Access Token (T1528)` `Use Alternate Authentication Material (T1550.001)`

Affected resources:

- r.veldman@domain.nl
- Microsoft Authentication Broker (29d9ed98-a469-4536-ade2-f981bc1d605e)
