EvilTokens Device Code Phishing Targets Microsoft 365 Accounts

***Author**: Portia S. Cole – CTI Researcher*

TL;DR

EvilTokens is a phishing-as-a-service platform that uses device-code authentication to compromise Microsoft 365 accounts.

Organizations should restrict this authentication method because a successful attack can give threat actors access to email, files and other cloud services.

Overview

EvilTokens targets Microsoft 365 users with phishing emails about invoices, shared documents, electronic signatures, voicemail messages or password expiration. The embedded link leads to an attacker-controlled page that displays a device code and sends the user to Microsoft's legitimate device-login website.

Entering the code authorizes the attacker's session. This gives the attacker authentication tokens that can be used to access the victim's account, even when multifactor authentication is enabled. The campaign abuses a legitimate Microsoft authentication process rather than exploiting a vulnerability or stealing passwords.

Affected Services

- Microsoft 365
- Microsoft Entra ID
- Microsoft Exchange Online and Outlook
- Microsoft SharePoint Online
- Microsoft OneDrive
- Microsoft Teams

Cisco Talos identified an EvilTokens affiliate panel called ARToken during an incident investigation. The panel allows operators to search Outlook mailboxes, create inbox rules, send emails through compromised accounts and access SharePoint and OneDrive files. It can also register devices to maintain access.

Talos also observed ARToken emails impersonating a vendor and targeting an accounts-payable employee at a U.S. life-sciences company. The emails used an outstanding-invoice lure and linked to an attacker-controlled SharePoint tenant that resembled the vendor's legitimate tenant. More than 1,000 phishing pages have been connected to the broader EvilTokens operation.

Aspire Protects

- Block device-code authentication through Microsoft Entra Conditional Access if it is not needed.
    - Review current use in report-only mode and limit exceptions to approved accounts and devices.
- Monitor Entra ID logs for unexpected device-code sign-ins, unfamiliar locations and new device registrations.
- Configure Microsoft Defender for Office 365 anti-phishing policies and Safe Links.
- Remind users not to enter device codes received through emails or document-sharing pages.
- If an account is compromised, disable it temporarily, revoke active sessions and refresh tokens, and remove unauthorized registered devices.
    - Review Outlook, SharePoint and OneDrive activity to determine what the attacker accessed.

TTPs to Watch

Initial Access

- Phishing: Spearphishing Link [T1566.002] – The attacker may send a link that directs the target to an EvilTokens phishing page.

Credential Access

- Steal Application Access Token [T1528] – The attacker may obtain Microsoft access and refresh tokens after the target completes the device-code authentication request.

Persistence

- Account Manipulation: Device Registration [T1098.005] – The attacker may register a device with the compromised account to maintain access.

Lateral Movement

- Use Alternate Authentication Material: Application Access Token [T1550.001] – The attacker may use stolen tokens to access Microsoft 365 services without the victim’s password.

Collection

- Email Collection: Email Forwarding Rule [T1114.003] – The attacker may create inbox rules to forward messages to an attacker-controlled account.
- Data from Cloud Storage [T1530] – The attacker may access files stored in SharePoint or OneDrive.

IoCs

Domains

- pamconj[.]com
- dashboard-bl[.]pamconj[.]com
- spx[.]pamconj[.]com
- clear90489058903-document[.]workers[.]dev
- reynoldsjace5[.]workers[.]dev

Hostnames

- 917bedb0-554e-a8b9-79f1-docviewer[.]clear90489058903-document[.]workers[.]dev
- 321a1392-939d-3bf5-4040-docviewer[.]clear90489058903-document[.]workers[.]dev
- 98c4c82e-2d81-0837-e3d6-docviewer[.]clear90489058903-document[.]workers[.]dev
- 112838d8-9a75-2e90-d63b-docviewer[.]clear90489058903-document[.]workers[.]dev
- aquaclaude-09494-9099403-docviewer[.]clear90489058903-document[.]workers[.]dev
- e5469cec-124a-c84f-abaa-docviewer[.]clear90489058903-document[.]workers[.]dev
- 50a201fd-dd2d-cf72-5fa6-onedrive[.]clear90489058903-document[.]workers[.]dev
- 50a201fd-dd2d-cf72-5fa6-adobe2[.]reynoldsjace5[.]workers[.]dev

IP Address

- 172[.]67[.]214[.]35

Note: The listed IP address and Cloudflare Workers infrastructure may also support legitimate activity. Organizations should **investigate matches before blocking** shared infrastructure.

Targeted Industries

The campaign targets Microsoft 365 users worldwide, particularly employees who handle financial transactions, employee information or sensitive business communications. Observed targeting includes:

- Life Sciences
- Logistics and Transportation

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

ARToken: Inside an EvilTokens affiliate panel targeting Microsoft 365

IR Trends Q2 2026: Phishing and weaponized remote management tools drive attack chains