Advisory Notice

Issue Date 20th February 2025

TLP: CLEAR

Information in this report has been given a Traffic Light Protocol (TLP) of CLEAR

CLEAR **Public** - May be distributed freely, without restriction.

Storm-2372: Targeting Microsoft Device Code Authentication

Overview

A new phishing campaign, attributed to a threat actor known as Storm-2372, is targeting Microsoft accounts across multiple sectors. Microsoft's Threat Intelligence Centre believes that Storm-2372 is linked to a nation-state operation that aligns with Russian interests, based on their tradecraft, victimology, and tactics.

Storm-2372's attack employs a phishing technique known as device code phishing, which exploits device code authentication flows. Devices often rely on a code-based system for users to sign into apps by entering an authentication code on a separate device.

Detail

The threat actor has been manipulating this authentication flow by tricking users into entering attacker-generated codes on legitimate sign-in pages. The attackers initially establish a connection with the victim by posing as a trusted figure, using messaging platforms to gain the target's trust.

The victim receives a Teams meeting invitation with a device code generated by the threat actor. When the victim clicks the invitation, they are prompted to authenticate via the device code. By entering this code, the victim unknowingly provides the attacker with a valid access token, which allows the actor to hijack the authenticated session and gain access to the victim's Microsoft services, such as email and cloud storage, without needing a password.

This technique grants the attacker access to the victim's accounts as long as the stolen tokens remain valid. In some cases, Microsoft has observed that the threat actor has used the specific Microsoft Authentication Broker client ID to generate new tokens, expanding their persistence and attack capabilities. This method allows the attackers to register devices to Microsoft Entra ID, enabling continued access to compromised accounts.

Recommended Action

- Restrict Device Code Flow: Block device code flow wherever possible and configure Microsoft Entra ID to limit it to trusted devices or networks through Conditional Access policies.
- Monitor Sign-in Logs: Use Microsoft Entra ID's sign-in logs to track suspicious activities.
- Enforce Multi-Factor Authentication (MFA): Require MFA to mitigate the impact of phishing attacks. Where possible, use phishing-resistant MFA methods, such as FIDO tokens or Microsoft Authenticator with passkeys.
- Monitor Authentication Risks: Implement sign-in risk policies in Conditional Access to automatically respond to suspicious login attempts based on the risk level associated with the sign-in
- Review Legacy Authentication: Disable legacy authentication protocols in Microsoft Entra ID, as they do not support MFA and are more susceptible to abuse.

Further Reading – Microsoft - Storm-2372 conducts device code phishing campaign | Microsoft Security Blog

If you have any concerns, or have been affected by a cyber-related issue, report it to the Cyber Security Centre by submitting a Cyber Concerns Online Reporting Form at https://csc.gov.im

TLP: CLEAR