THREAT BULLETINS

Storm-2372 Conducts Device Code Phishing Campaign

TLP:WHITE

Feb 14, 2025

The Microsoft Threat Intelligence Center has identified an active device code phishing campaign conducted by a group known as Storm-2372, which has been operational since August 2024. This threat actor targets various sectors, including government, NGOs, IT, defense, telecommunications, health, education, and energy across Europe, North America, Africa, and the Middle East. Microsoft has assessed with medium confidence that this threat actor might be linked to Russia.

The campaign includes sending phony meeting invitations via email, mimicking Microsoft Teams, and prompting users to authenticate using a device code generated by the threat actor. Once a victim authenticates, the attackers leverage the obtained access tokens to infiltrate the network further.

For more information, including mitigation guidance, please see the full Microsoft report here. This alert is shared for your situational awareness as this threat actor previously targeted the health sector.

Reference(s)	Microsoft Blog

Incident Date
Feb 14, 2025 (UTC)

Alert ID 03ac2973

View Alert

Share Feedback

was this helpful? |

Tags Microsoft Threat Intelligence Center, Storm-2372

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments
Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**