Alert Bulletin

Bulletin N.: 2024-55
Publication Date: 18/10/2024
Subject: Alert 2024-55: Fénix Botnet Active in Mexico
Traffic Light Protocol (TLP): White

The criminal group managing the Fénix botnet has intensified its activities since 2022. This botnet has carried out multiple attacks, primarily targeting the SAT (Tax Administration Service), using phishing and fraudulent websites mimicking official portals as attack vectors, thus demonstrating a strong focus on Mexican citizens.

These fake sites prompt users to download files allegedly intended to improve security when navigating the portal. However, the download installs the initial stage of the malware, allowing the attacker to access confidential information, such as login credentials.