Scottish Cyber Coordination Centre

Daily Threat Bulletin

18 February 2025

Vulnerabilities

Xerox Versalink Printer Vulnerabilities Enable Lateral Movement

SecurityWeek - 17 February 2025 12:00

Xerox released security updates to resolve pass-back attack vulnerabilities in Versalink multifunction printers.

Threat actors and malware

New FinalDraft Malware Spotted in Espionage Campaign

SecurityWeek - 17 February 2025 14:39

A newly identified malware family abuses the Outlook mail service for communication, via the Microsoft Graph API.

Microsoft Uncovers New XCSSET macOS Malware Variant with Advanced Obfuscation Tactics

The Hacker News - 17 February 2025 23:00

Microsoft said it has discovered a new variant of a known Apple macOS malware called XCSSET as part of limited attacks in the wild."Its first known variant since 2022, this latest XCSSET malware features enhanced obfuscation methods, updated persistence mechanisms, and new infection strategies.

Pro-Russia collective NoName057(16) launched a new wave of DDoS attacks on Italian sites

Security Affairs - 17 February 2025 11:14

Pro-Russia collective NoName057(16) launched DDoS attacks on Italian sites, targeting airports, the Transport Authority, major ports, and banks. The pro-Russia hacker group NoName057(16) launched a new wave of DDoS attacks this morning against multiple Italian entities.

Telegram Used as C2 Channel for New Golang Malware

Infosecurity Magazine - 17 February 2025 12:15

A Golang backdoor is using Telegram as its command and control (C2) channel, an approach that makes detection harder for defenders, according to Netskope researchers