مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

New FrigidStealer Infostealer Targeting macOS Users

Tracking #:432316890

Date:20-02-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a new macOS infostealer called FrigidStealer, targeting users through fake browser update campaigns.

TECHNICAL DETAILS:

A new macOS infostealer malware, named FrigidStealer, is being distributed through FakeUpdate campaigns. These campaigns deceive users into downloading malicious software by displaying fake browser update alerts. This malware is part of a larger operation involving two cybercrime groups, TA2726 and TA2727, which also distribute malware for Windows and Android devices.

FrigidStealer Campaign

FrigidStealer is delivered to Mac users via compromised websites that display fake browser update notifications. The campaign works as follows:

1. Malicious JavaScript is injected into legitimate websites.
2. Users are shown fake update prompts for browsers like Safari or Chrome.
3. Clicking the "Update" button downloads a DMG file containing FrigidStealer.
4. Users are instructed to bypass macOS Gatekeeper by right-clicking and selecting "Open"

Malware Capabilities:

FrigidStealer is a Go-based malware built with the WailsIO framework to appear legitimate. Once installed, it:

- Extracts cookies, login credentials, and password-related files from Safari and Chrome.
- Scans for cryptocurrency wallet credentials in Desktop and Documents folders.
- Collects sensitive information from Apple Notes.
- Gathers documents, spreadsheets, and text files from the user's home directory.

The stolen data is exfiltrated to a command and control server at 'askforupdate[.]org'.

Threat Actors

Two new cybercrime groups are involved in this campaign:

1. TA2726: Active since September 2022, acts as a traffic distributor and facilitator.
2. TA2727: First identified in January 2025, responsible for distributing FrigidStealer (macOS), Lumma Stealer (Windows), and Marcher (Android).

Indicators of Compromise (IOC):

Attached File

RECOMMENDATIONS:

- Never download or execute software updates from unverified websites.
- Be cautious of any unexpected browser update notifications.
- Keep operating systems and browsers updated through official channels only.
- Use robust antivirus and anti-malware solutions.
- Implement strong, unique passwords for each account and use a password manager.
- Enable two-factor authentication where possible.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.proofpoint.com/us/blog/threat-insight/update-fake-updates-two-new-actors-and-new-mac-malware