مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Malware Campaign- New "RustDoor" Backdoor Targeting macOS

Tracking #:432315607

Date:12-02-2024

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed New "RustDoor" Backdoor Targeting apple macOS systems.

## TECHNICAL DETAILS:

Apple macOS users are being targeted by a new Rust-based backdoor called RustDoor, which has been operating since November 2023.

The backdoor is distributed as FAT binaries that contain Mach-O files and impersonates an update for Microsoft Visual Studio. It targets both Intel and Arm architectures, and the exact initial access pathway used to propagate the implant is currently unknown. Multiple variants of the malware with minor modifications have been detected, indicating active development.

RustDoor comes with a wide range of commands that allow it to gather and upload files, and harvest information about the compromised endpoint. Some versions also include configurations with details about what data to collect, the list of targeted extensions and directories, and the directories to exclude. The captured information is then exfiltrated to a command-and-control (C2) server.

The malware is likely linked to prominent ransomware families such as Black Basta and BlackCat due to overlaps in C2 infrastructure. This threat, observed as Trojan.MAC.RustDoor, leverages the Rust programming language.

## INDICATORS OF COMPROMISE(IoCs):

- Attached in Excel File

## RECOMMENDATIONS:

- Block the attached IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Use reputable anti-malware software and regularly scan systems for malware, including ransomware.
- Avoid downloading software from untrusted sources and be cautious of suspicious emails or messages.
- Keep all of your software's up to date with latest patches, including macOS.
- Use strong passwords with multi-factor authentication (MFA).

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings (e.g. IOCs, TTPs...etc).

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

## REFERENCES:

1. https://www.bitdefender.com/blog/labs/new-macos-backdoor-written-in-rust-shows-possible-link-with-windows-ransomware-group/