مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

DuneQuixote Campaign Targets Middle East with CR4T Malware

Tracking #:432315776

Date:22-04-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council observed a malicious campaign targeting organizations in the Middle East with a backdoor Trojan called CR4T.

TECHNICAL DETAILS:

A new malware campaign, dubbed DuneQuixote, has been discovered targeting government entities in the Middle East. This campaign involves the use of dropper samples that deploy the CR4T malware. The campaign has been active since at least February 2024, with over 30 dropper samples identified.

Campaign Overview:
Campaign Name: DuneQuixote
Targets: Entities in the Middle East
Malware: CR4T backdoor (C/C++ and Golang variants)
Delivery Methods:

- Droppers disguised as legitimate software (e.g., tampered Total Commander installer)
- Droppers download the CR4T backdoor after compromising a system.

CR4T Backdoor Capabilities:

- Remote console access for attackers
- File download and upload functionalities
- Golang variant can execute commands and schedule tasks

Impact: Successful infection allows attackers to steal sensitive data, manipulate files, and potentially gain further access within the network.

Indicators of Compromise:
Attached 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.
- Strengthen Security Measures: Implement robust security measures, including firewalls, intrusion detection systems, and antivirus software, to protect against the DuneQuixote campaign and CR4T malware.
- Monitor Network Traffic: Increase monitoring of network traffic and system logs for any suspicious activities that could indicate exploitation of the DuneQuixote campaign.
- Regularly Update Software: Keep all software and systems up-to-date with the latest security patches and updates.

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://securelist.com/dunequixote/112425/