مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Windows SmartScreen Vulnerability Exploited in DarkGate Malware Attacks

Tracking #:432315708
Date:18-03-2024

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed the Windows SmartScreen Vulnerability has been exploited in DarkGate malware attacks, posing a significant threat to systems

## TECHNICAL DETAILS:

The Windows SmartScreen Vulnerability has been exploited in DarkGate malware attacks, posing a significant threat to systems. This vulnerability, identified as CVE-2024-21412, allows attackers to bypass security measures and drop the DarkGate malware, potentially leading to unauthorized access, data compromise, and system infiltration.

- Vulnerability: CVE-2024-21412 (Windows Defender SmartScreen Bypass)
- Impact: Allowed attackers to bypass SmartScreen warnings and deploy malicious software (DarkGate malware) disguised as legitimate software installers.
- Exploitation:
  - Malicious actors sent phishing emails with PDF attachments containing links.
  - These links used open redirects from Google services to compromised servers.
  - Compromised servers hosted specially crafted shortcut files (.url) exploiting the vulnerability.
  - Clicking the shortcut bypassed SmartScreen and downloaded fake installers containing DarkGate.
- Resolution: Microsoft patched the vulnerability in February 2024 updates.

## INDICATORS OF COMPROMISE(IoCs):

Attached 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.

- Ensure that systems are up-to-date with the latest security patches. including the fix for CVE-2024-21412.
- Be cautious of unexpected emails with attachments, especially those urging software downloads.
- Only download software from trusted sources and official websites.

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.trendmicro.com/en_us/research/24/c/cve-2024-21412--darkgate-operators-exploit-microsoft-windows-sma.html