مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

TrickMo Android Banking Trojan

Tracking #:432316398

Date:16-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

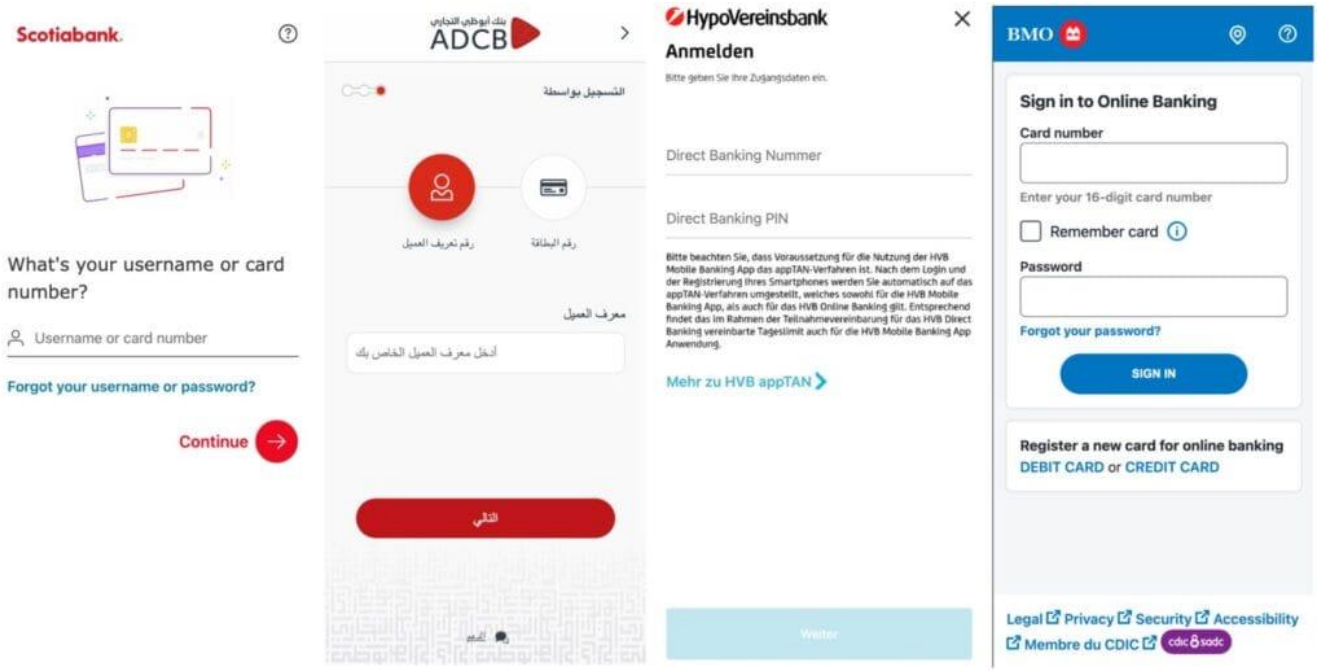
The UAE Cyber Security Council has observed a sophisticated variant of the TrickMo banking Trojan that is actively targeting Android devices in a recent campaign.

TECHNICAL DETAILS:

Security researchers have discovered an advanced variant of the TrickMo banking Trojan specifically aimed at Android devices. This malware exhibits advanced anti-analysis mechanisms, including the use of malformed ZIP files and JSONPacker, complicating detection and analysis efforts. The malware is distributed via a dropper app disguised as a legitimate application, exploiting user trust to gain elevated permissions. The findings reveal significant risks, including banking fraud, identity theft, and data leakage, underscoring the need for robust cybersecurity measures.

Overview of TrickMo:
TrickMo is an Android banking Trojan that has evolved from the TrickBot malware family. Its capabilities include:

- **Interception of One-Time Passwords (OTPs)**: Bypasses two-factor authentication (2FA) mechanisms.
- **Screen Recording and Keylogging**: Captures sensitive information from users.
- **Remote Control Capabilities**: Allows attackers to manipulate infected devices without user consent.



Deceptive overlays

TrickMo employs sophisticated techniques to evade detection, including:

- Dropper Applications: Disguised as legitimate apps (e.g., Google Chrome), these dropper apps install the TrickMo malware while prompting users to enable accessibility services.
- Advanced Obfuscation Techniques: The use of malformed ZIP files and JSONPacker complicates analysis efforts by security professionals.
- Command-and-Control Communication: The malware communicates with its C2 server using HTTP requests to exfiltrate data and receive commands, allowing continuous control over infected devices.

Risks Associated with Data Leakage:

The exposed data from the C2 infrastructure poses significant risks:

- Identity Theft: Stolen personal documents can be used to create fake identities or bypass security checks.
- Financial Fraud: Access to banking credentials enables direct theft or unauthorized transactions.
- Targeted Phishing Attacks: Compromised information can be leveraged for highly convincing phishing schemes.

Geolocation Findings:

The analysis of IP addresses from the compromised C2 servers indicates a significant concentration of victims in the following countries:

- Canada
- United Arab Emirates
- Turkey
- Germany

INDICATORS OF COMPROMISE(IOCs):

Attached in Excel File

RECOMMENDATIONS:

- Review the Indicators of Compromise (IOCs) and implement the necessary security measures.
- Utilize Intrusion Detection Systems (IDS) to monitor network traffic for unusual activities associated with known malicious IP addresses.
- Enhance Endpoint Security: Deploy advanced endpoint protection solutions that can detect and respond to mobile threats like TrickMo.

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.cleafy.com/cleafy-labs/a-new-trickmo-saga-from-banking-trojan-to-victims-data-leak