Subject:- **Analysis Report Phishing Based Advanced Persistent Threat (APT) Targeting Intelligence Bureau Division's (IBD) Officers (Advisory No. 08)**

Recently, an Advanced Persistence Threat (APT) campaign has been observed targeting the Intelligence Bureau Division's (IBD) officers through phishing attacks. The attackers aimed to steal sensitive information from the computers under the use of IB officers. On 30-04-2024, IBD HQ identified a suspicious file named "2nd NAP Coordination Committee Meeting.rar" file through WhatsApp message. The attacker impersonated as a NACTA official and sent messages to IBD HQ's Senior Officer from WhatsApp number 03557876530.

2. Upon inquiry, the CMO Special Communication Organization (SCO) informed that the WhatsApp number does not exist in their record. Few details are attached as **Annex-A**.

3. **Identified Malware Capabilities**. There were two malicious zip files identified as under:

a. Minutes of second NAP CCM.pdf.chm
b. SearchApp.exe.

4. Second file is the windows hidden executable file created to execute on opening of the first file a malicious code on the target Operating system. Initial analysis suggests the presence of information-stealing malware. This type of malware can:

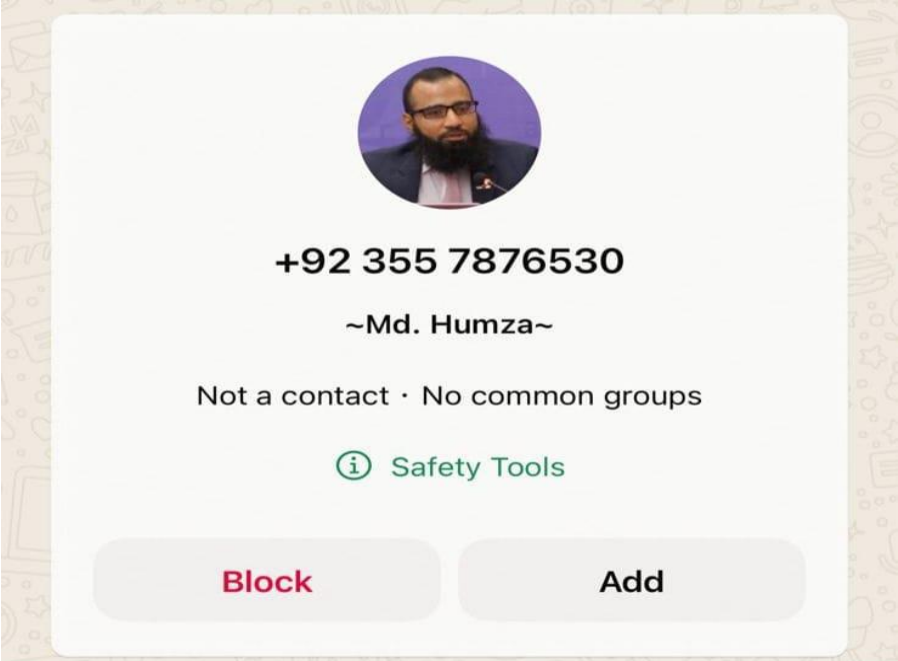
a. Capture keystrokes, including login credentials and sensitive documents.
b. Take screenshots of user activity.
c. Exfiltrates files from the compromised devices through secure encrypted channel and Command & Control Server.
d. Malware contacts the Linux based Command-and-Control server hosted by M247 Europe SRL to covert data transfer through encrypted (SSL) channels. Details are as under:
    (1) **IP Address:** 162.252.175.170 Ports: 22, 3389, 443 (used for malware communication).
    (2) **Company:** M247 Europe SRL is a hosting and cloud services provider.

5. **Potential Impacts**. The above attack poses a significant threat as attacker aimed to steal the sensitive data from the computers used by the Senior Government Officers.

6. **Recommendations**. All Government Officials are advised to adopt cautious approach and do not use WhatsApp for official correspondence specially sharing of official documents. Official documents received on WhatsApp as well as on email, be double checked from sender for authenticity.

Annex-A

WhatsApp Profile of the Attacker



Malware Analysis

Detection using Machine Learning and Static Analysis Results Indicators of Compromise

Malicious Indicators

External Systems

Sample detected by CrowdStrike Static Analysis and ML with relatively high confidence

details CrowdStrike Static Analysis and ML (QuickScan) yielded detection: win/malicious_confidence_100% (W)
source External System
relevance 10/10

Contacted Hosts

Login to Download Contacted Hosts (CSV)

IP Address	Port/Protocol	Associated Process	Details
162.252.175.170	443 TCP	searchapp.exe PID: 904	United States

Contacted Countries