Mil Tele: 6130
Civ Tele : 0172-2589145

AWES Cell
Headquarters
Western Command
Chandimandir-134 107

46353/ Cyber/AWES

28 Jun 2022

List A (AWES)

ADVISORY ON SUSPICIOUS MALWARE ON WHATSAPP TO IA PERS (ADVISORY NO 16/2022)

1. Photocopy of HQ Western Comd letter No 47722/Cyber/A5 dt 25 Jun 2022 is fwd herewith.

2. You are requested to instr all Schools and Colleges under your jurisdiction, to promulgate the subject advisory and take necessary counter measures.

(RS Bhatti)
Col (Retd)
Dir (AWES)
for MG IC Adm

Copy to :-

(All APSs & Colleges) - for necessary action wrt above pl.

RESTRICTED

Tele: 2644

HQ Western Comd
PIN-908543
c/o 56 APO

18042/PIO/advisory/GSI (C)

22 Jun 2022

List A & F

ADVISORY ON SUSPICIOUS MALWARE ON WHATSAPP TO IA PERS (ADVISORY NO 16/2022)

1. **Gen**. An advisory on suspicious malware on WhatsApp to IA pers recd from DGMI/MMI-9 is given in succeeding paras.

(a) It has been reported by an int agency that two malwares namely **'Update Portal.vhdx'** & **'Student Online Update Portal.apk'** are being circulated by a suspicious WhatsApp No **+917603847882** (Screenshot of the WhatsApp conv showing receipt of malware is att as **Appx** A). The a/m malware is tgt IA pers whose children are studying in APS.

(b) **Social Engg Theme**. An innovative social engg theme being utilized in **'update on PTM/Fee structure/Exam result/New syllabus/ Student record/ New classes sch in new version of Digicamps'**. The APS use Digicamp online app to host their data. The malwares lure the user as an update to the Digicamp app.

(c) **Analysis**. The analysis of the a/m input has revealed that the a/m suspicious WhatsApp No is being operated from an IP add **geo-located in Karachi**. The infected digital devices indicate that they are communicating with the C2 server based at a/m loc.

(d) In view of the above fwg actions may be taken by the users:-

(i) The user must login through NIC servers having **'https'** verification.

(ii) Links recd on emails or other platforms should not be clicked.

(iii) In case of any suspicious obsn, change of password option must be exercised by the user imdt.

(iv) All users may be sensitized about a/m spear phishing attacks made to steal the data and instr to restrict all comn.

2. **Promulgation**. The a/m advisory be to promulgated to all units/fmns/Br running the schools in stn and all concerned institutions to take necessary counter measures.

3. For wide dissemination pl.

(Gurinder Singh)
Col
SO (Int)
for COS

Copy to :-

DGMI/MI-9 - for info wrt letter No A/38024/MI-11 (ii) dt 10 Jun 22.

RESTRICTED