

Subject:- **Cyber Security Advisory - Notification of IP addresses Potentially Targeted with Sophisticated Malware (Advisory No. 30)**

Reportedly, some threat actors are targeting users for data acquisition through a highly sophisticated Malware. Following suspicious Pakistani URLs may be potential targets: -

Serial	IP/URL	ISP/Hosting
a.	202.63.219.133	CubeXS, Karachi
b.	202.63.219.134	CubeXS, Karachi
c.	203.101.170.4	CyberNet, Karachi
d.	66.45.251.115	Interserver, New York
e.	66.45.251.120	-
f.	Fashionmasala.pk	-
g.	Agspharmas.com	-

2. Above in view, users/administrators are requested to adhere to the following recommendations: -

- a. Monitoring of the mentioned IP addresses/domains at SOC.
- b. Processing of Cyber investigation, in case, any system/device is found communicating with aforementioned addresses.
- c. Outcome of the investigation may be shared with this organization for evaluation and assistance (if required) via email ID: falconl947@proton.me.