Pakistan Telecommunication Authority
Headquarters, Islamabad

PTA Cyber Security Advisory No.: 155 **24-08-2022**

Name: APT group from India, Confucius, targeting Pakistani embassies in multiple countries

Threat Classification: Phishing Emails, APT Group

Summary:

A Threat Intelligence was received from Avast CERT Team, where they discovered a known APT group from India, Confucius, targeting Pakistani embassies in multiple countries like Brunei, Nepal, Argentina, and Azerbaijan from March to June 2022. The Confucius group spread their malware by sending phishing emails with PDF attachments, which contained links to phishing websites. These sites imitated official government websites which contained passwords for documents site visitors could download, these documents were malicious. This is done so that the files remain encrypted, to avert detection from static AV scanners. They spotted malicious documents with various names related to current events, such as "**VaccineStatusReport.xlsx**".

The group used documents with malicious macros to drop further infection stages written in C#. It is also noticed that several other malware families like trojan downloaders, file stealers, QuasarRAT and a custom RAT developed in C++ being dropped by the macros. It is suspected that the group may be after intelligence, based on the fact that the malware being used in the attacks is designed to spy on victims and steal files and other data.

Recommendations:

1. Avoid tempting or threatening content in the email
2. Don't click on unknown links in emails. These can be malicious
3. Always check complete email address of sender
4. Be careful with attachments especially with extensions like .xlsx, .xls, pdf, doc, docx .exe, .msi, .vb, .bat etc
5. Train employees on phishing, social engineering and incident response procedures
6. Ensure 24/7 security monitoring of critical infrastructure, services, and websites for proactive remediation and response to any detected/observed abnormal activity.
7. Report suspicious email addresses to your respective organizations
8. If any malicious activity is found immediately inform PTA through the CERT portal or email at cert@pta.gov.pk