**Cyber Security Advisories**

**Date: 17 June 2024**

**Name of Control Centre:**

| **S No** | **Vulnerability Note No** | **Applicable to Organisation** | **If Yes: Action Taken:** | **Remarks** |
| --- | --- | --- | --- | --- |
| **(Yes/No)** | **Yes / No/ Deferred** |
|  | CMTX-I-514052024 Threat Actors using Google Drive Based Services for Data Exfiltration |  |  |  |
|  | CMTX-I-200052024 CrimsonRAT - APT36 campaign |  |  |  |
|  | CMTX-I-040052024 SpyNote -  APT36 Campaign |  |  |  |
|  | CMTX-P062024726 QuasarRAT Malware ALERT 54 |  |  |  |
|  | CMTX-P062024405 PLUGX RAT ALERT 120 |  |  |  |
|  | CMTX-P-062024015 Asylum Ambuscade Group |  |  |  |
|  | CMTX-I-050152024 Malicious Domains used by APT Threat Actors |  |  |  |
|  | CMTX-I-040152024 Malicious Domains used by APT Threat Actors |  |  |  |
|  | CMTX-I-050152024 Malicious Domains used by APT Threat Actors |  |  |  |
|  | CMTX-I-050152024 Malicious Domains used by APT Threat Actors |  |  |  |
|  | CMTX-I-445062024 Mythic Malware - APT36 campaign |  |  |  |
|  | CMTX-I-053062024 Recent IOCs of Chinese Malware Campaign |  |  |  |
|  | CMTX-I-004002024 Domains associated with ReverseRAT Malware |  |  |  |
|  | CMTX-I-022062024 CrimsonRAT - APT36 campaign |  |  |  |
|  | CMTX-P062024985 SHADOWPAD Malware |  |  |  |
|  | CMTX-P062024995 SHADOWPAD Malware |  |  |  |
|  | CMTX-P062024505 PLUGX RAT ALERT 121 |  |  |  |
|  | CMTX-P062024025 Cyber Espionage by Chinese Threat Actors |  |  |  |
|  | CMTX-I-025062024 Malicious Domains - Spear-Phishing Campaign |  |  |  |
|  | CMTX-I-443062024 Malicious Domains - Spear-Phishing Campaign |  |  |  |
|  | CMTX-I-080062024 SideCopy - C&C of Malware Campaign |  |  |  |
|  | CMTX-I-808062024 Malicious Domains - Spear-Phishing Campaign |  |  |  |
|  | CMTX-I-543062024 Malicious Domains - Spear-Phishing Campaign |  |  |  |
|  | CMTX-P062024018 REDLINE STEALER MALWARE |  |  |  |