**Cyber Security Advisories**

**Date: 30 August 2024**

**Name of Control Centre:**

| **S No** | **Vulnerability Note No** | **Applicable to Organisation** | **If Yes: Action Taken:** | **Remarks** |
| --- | --- | --- | --- | --- |
| **(Yes/No)** | **Yes / No/ Deferred** |
|  | CMTX-P-082024094 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-0820240704 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-995082024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P082024062 Dispossessor Ransomware |  |  |  |
|  | CMTX-P082024007 SystemBC Malware Campaign |  |  |  |
|  | CMTX-I-514082024 SideCopy Malware C&C IP |  |  |  |
|  | CMTX-P082024095 QWERTY INFO STEALER |  |  |  |
|  | CMTX-P082024104 Beavertail Malware Campaign |  |  |  |
|  | CMTX-P-5870820249 Threat Actor Group-110 (TAG 110) Recent IOCs |  |  |  |
|  | CMTX-I-445082024 CrimsonRAT Malware C&C IP |  |  |  |
|  | CMTX-P082024115 CVE-2024-38193 |  |  |  |
|  | CMTX-I-587082024 Suspicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-765082024 Malicious Domain used by Pakistan based Threat Actors |  |  |  |
|  | CMTX-P082024956 Styx Stealer |  |  |  |
|  | CMTX-I-995082024 Malicious/ Suspicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P-082024114  RedJuliett Threat Actor Campaign |  |  |  |
|  | CMTX-P-082024125 STORMBAMBOO THREAT ACTOR CAMPAIGN |  |  |  |
|  | CMTX-P082024108 REDLINESTEALER Malware Campaign |  |  |  |
|  | CMTX-P-082024135 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-082024145 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-I-680082024 CrimsonRAT- APT36 campaign |  |  |  |
|  | CMTX-I-636082024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-179082024 CrimsonRAT- APT36 campaign |  |  |  |
|  | CMTX-I-432082024 Android RAT Latest C&C IP |  |  |  |
|  | CMTX-P-082024155 VELVETSHELL MALWARE |  |  |  |
|  | CMTX-P082024834 MoonPeak Malware Campaign |  |  |  |
|  | CMTX-I-781082024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P082024976 QuasarRAT Malware |  |  |  |
|  | CMTX-P082024664 Ransom Hub Ransomware |  |  |  |
|  | CMTX-P082024165 ACTIVE EXPLOITATION OF PUBLIC FACING APPLICATION VULNERABILITIES BY IRANIAN THREAT ACTORS |  |  |  |
|  | CMTX-I-950082024 QuasarRAT- Deployed by Pakistan based Threat Actors |  |  |  |