**Cyber Security Advisories**

**Date: 28 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-338062024 SideCopy - IOCs of Malware Campaign |  |  |  |
|  | CMTX-P062024605 PLUGX RAT ALERT 122 |  |  |  |
|  | CMTX-P062024105 SHADOWPAD Malware |  |  |  |
|  | CMTX-P062024736 QuasarRAT Malware |  |  |  |
|  | CMTX-P062024045 Circulation of Phishing email contain links to counterfeit CERT-In websites |  |  |  |
|  | CMTX-I-345062024 Malicious Domains - Spear-Phishing Campaign |  |  |  |
|  | CMTX-P062024065 Velvet ant Threat Actor |  |  |  |
|  | CMTX-P062024028 RACCOON MALWARE |  |  |  |
|  | CMTX-I-808062024 Malicious Domains - Spear-Phishing Campaign |  |  |  |
|  | CMTX-I-338062024 SideCopy - IOCs of Malware Campaign |  |  |  |
|  | CMTX-P062024055 CRITICAL VULNERABILITY (CVE-2024-30103) AFFECTING MICROSOFT OUTLOOK |  |  |  |
|  | CMTX-I-021062024 Malicious Domains - Spear-Phishing Campaign |  |  |  |
|  | CMTX-P062024075 ACTIVE EXPLOITATION OF A CRITICAL VULNERABILITY (CVE-2024-28995) AFFECTING SOLAR WINDS SERV-U FILE TRANSFER SOFTWARE |  |  |  |
|  | CMTX-I-555062024 Mythic Malware - APT36 campaign |  |  |  |
|  | CMTX-P062024085 MYTHIC MALWARE |  |  |  |
|  | CMTX-P062024105 Pantegana Malware |  |  |  |
|  | CMTX-P062024038 Agent Tesla Malware Alert |  |  |  |
|  | CMTX-P062024048 Amadey Malware Alert |  |  |  |
|  | CMTX-P062024058 Emotet Malware |  |  |  |
|  | CMTX-P062024068 Qbot Malware |  |  |  |
|  | CMTX-P062024078 RACCOON MALWARE |  |  |  |
|  | CMTX-P062024088 Redline malware |  |  |  |
|  | CMTX-P062024098 SocGholish malware |  |  |  |
|  | CMTX-P062024108 Trickbot malware |  |  |  |
|  | CMTX-P062024118 Ursnif malware |  |  |  |
|  | CMTX-P-062024115 DEPLOYMENT OF CL0P RANSOMWARE VARIANT BY FIN7 CYBERCRIMINAL GROUP |  |  |  |
|  | CMTX-P06024125 SparkRAT Malware |  |  |  |
|  | CMTX-I-911062024 Malicious Domains - Spear-Phishing Campaign |  |  |  |
|  | CMTX-I-389062024 IOCs of Pakistan based Malware Campaign |  |  |  |
|  | CMTX-P062024135 MYTHIC MALWARE |  |  |  |
|  | CMTX-I-433062024 Malicious Domains - Spear-Phishing Campaign |  |  |  |
|  | CMTX-P062024756 QuasarRAT Malware ALERT 56 |  |  |  |
|  | CMTX-P062024746 GH0ST RAT Malware |  |  |  |
|  | CMTX-I-090062024 Malicious Domains used by Pakistan based Threat Actors |  |  |  |
|  | CMTX-I-514062024 IOCs of APT36 Malware campaign |  |  |  |
|  | Adv/2024/Jun/024 Underground Team Ransomware |  |  |  |
|  | Adv/2024/Jun/025 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | Adv/2024/Jun/026 Phishing Attack |  |  |  |
|  | Adv/2024/Jun/027 ShrinkLocker Ransomware |  |  |  |
|  | Adv/2024/Jun/028 Asylum Ambuscade Group |  |  |  |
|  | Adv/2024/Jun/029 Threat Actor Velvet ant |  |  |  |
|  | Adv/2024/Jun/030 Critical Vulnerability in Microsoft Outlook |  |  |  |
|  | Adv/2024/Jun/031 QuasarRAT Malware |  |  |  |
|  | Adv/2024/Jun/032 RedLine Stealer |  |  |  |
|  | Adv/2024/Jun/033 Racoon Malware |  |  |  |
|  | Adv/2024/Jun/036 Lucky Ransomware Targeting Critical Sectors |  |  |  |
|  | Adv/2024/Jun/037 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | Adv/2024/Jun/038 FIN7 Cybercrime Group Deploys New CL0P Ransomware Variants |  |  |  |
|  | Adv/2024/Jun/039 Phishing Attack |  |  |  |