**Cyber Security Advisories**

**Date: 31 May 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-506052024 CrimsonRAT - APT36 campaign |  |  |  |
|  | CMTX-P052024085 Possible Exploitation of Public Facing Industrial Control Systems (ICSs) |  |  |  |
|  | CMTX-I-509052024 Android RAT - Cumulative IOCs |  |  |  |
|  | CMTX-P052024975 SHADOWPAD Malware |  |  |  |
|  | CMTX-P052024305 PLUGX RAT ALERT 119 |  |  |  |
|  | CMTX-P052024716 QuasarRAT Malware ALERT 53 |  |  |  |
|  | CMTX-I-515052024 IOCs of Android and NanoCore RAT |  |  |  |
|  | CMTX-P052024095 APT41 Chinese Threat Actor Activity |  |  |  |
|  | CMTX-I-410052024 CrimsonRAT - APT36 campaign |  |  |  |
|  | CMTX-P052024168 Trickbot malware |  |  |  |
|  | CMTX-P052024188 Agent Tesla Malware Alert |  |  |  |
|  | CMTX-P052024158 SocGholish malware |  |  |  |
|  | CMTX-P052024198 Amadey Malware Alert |  |  |  |
|  | CMTX-P052024208 REDLINE STEALER MALWARE |  |  |  |
|  | CMTX-P052024178 Ursnif malware |  |  |  |
|  | CMTX-P052024148 Emotet Malware |  |  |  |
|  | CMTX-P-052024105 ShrinkLocker Ransomware |  |  |  |
|  | Adv/2024/May/040 Malicious IOCs |  |  |  |
|  | Adv/2024/May/041 Malicious IOCs related to KeyPlug & ShadowPad Malware |  |  |  |
|  | Adv/2024/May/042 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | Adv/2024/May/043 Zero Day Vulnerability in QNAP QTS (CVE-2024-27130) |  |  |  |
|  | Adv/2024/May/044 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | Adv/2024/May/045 CVE - KB Correlation, May 2024 |  |  |  |
|  | Adv/2024/May/047 Phishing Domains |  |  |  |
|  | Adv/2024/May/048 Malicious IOCs |  |  |  |
|  | Adv/2024/May/049 GH0ST RAT Malware |  |  |  |
|  | Adv/2024/May/050 RedLine Stealer |  |  |  |
|  | Adv/2024/May/051 Racoon Malware |  |  |  |
|  | Adv/2024/May/052 Threat Actor BlackTech |  |  |  |
|  | Adv/2024/May/053 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | Adv/2024/May/054 Racoon Malware |  |  |  |
|  | Adv/2024/May/055 RedLine Stealer |  |  |  |
|  | Adv/2024/May/056 NJRAT Malware |  |  |  |
|  | Adv/2024/May/057 GH0ST RAT Malware |  |  |  |
|  | Adv/2024/May/058 QuasarRAT Malware |  |  |  |
|  | Adv/2024/May/061 VacBan Stealer |  |  |  |
|  | Adv/2024/May/062 Active Exploitation of Cross Site Scripting (XSS) Vulnerability in LiteSpeed Cache Plugin for WordPress |  |  |  |
|  | Adv/2024/May/063 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | Adv/2024/May/064 Malicious IOCs |  |  |  |
|  | Adv/2024/May/065 Linux Poseidon Malware |  |  |  |
|  | Adv/2024/May/066 Phishing Attack |  |  |  |
|  | Adv/2024/May/068 Weekly Mirai Activity Report |  |  |  |