**Cyber Security Advisories**

**Date: 22 May 2024**

**Name of Control Centre:**

| **S No** | **Vulnerability Note No** | **Applicable to Organisation** | **If Yes: Action Taken:** | **Remarks** |
| --- | --- | --- | --- | --- |
| **(Yes/No)** | **Yes / No/ Deferred** |
|  | Adv/2024/May/001 Weekly Mirai Activity Report |  |  |  |
|  | Adv/2024/May/002 Phishing Attack |  |  |  |
|  | Adv/2024/May/003 Malicious IOCs |  |  |  |
|  | Adv/2024/May/004 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | Adv/2024/May/005 Malicious IOCs |  |  |  |
|  | Adv/2024/May/006 Hacktivists Targeting Operational Technology (OT) Devices |  |  |  |
|  | Adv/2024/May/007 Security Updates in Google Chrome |  |  |  |
|  | Adv/2024/May/008 Secure by Design Alert Eliminating Directory Traversal Vulnerabilities in Software |  |  |  |
|  | Adv/2024/May/009 Multiple Vulnerabilities in CyberPower's Equipment |  |  |  |
|  | Adv/2024/May/010 Exploitation of a Weakness in NetNTLM Authentication Protocol |  |  |  |
|  | Adv/2024/May/011 Phishing Domains |  |  |  |
|  | Adv/2024/May/012 Malicious IOCs |  |  |  |
|  | Adv/2024/May/013 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | Adv/2024/May/014 DarkBeatC2 – Latest MuddyWater Attack Framework |  |  |  |
|  | Adv/2024/May/015 ArcaneDoor Campaign |  |  |  |
|  | Adv/2024/May/016 Gold Digger Malware |  |  |  |
|  | Adv/2024/May/017 Phishing Attack |  |  |  |
|  | Adv/2024/May/018 Malicious IOCs |  |  |  |
|  | Adv/2024/May/019 Critical Vulnerabilities & Security Updates in Multiple Products |  |  |  |
|  | Adv/2024/May/020 Phishing Attack using KUTAKI Malware |  |  |  |
|  | Adv/2024/May/021 Phorpiex botnet distributes LockBit ransomware |  |  |  |
|  | Adv/2024/May/022 Banking Trojan - CarnavalHeist |  |  |  |
|  | Adv/2024/May/023 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | Adv/2024/May/024 Phishing Attack |  |  |  |
|  | Adv/2024/May/025 Malicious IOCs |  |  |  |
|  | Adv/2024/May/026 Weekly Mirai Activity Report |  |  |  |
|  | Adv/2024/May/027 The Cuttlefish Malware |  |  |  |
|  | Adv/2024/May/028 Threat Actors Abusing Microsoft API- Graph Facility |  |  |  |
|  | Adv/2024/May/029 Critical Vulnerabilities & Security Updates in Multiple Products |  |  |  |
|  | Adv/2024/May/030 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | Adv/2024/May/031 Transparent Tribe AKA APT36 |  |  |  |
|  | Adv/2024/May/032 Black Basta Ransomware |  |  |  |
|  | Adv/2024/May/033 Vulnerability in DigiWin EasyFlow .NET |  |  |  |
|  | Adv/2024/May/034 Kapeka Malware |  |  |  |
|  | Adv/2024/May/035 Mustang Panda |  |  |  |
|  | Adv/2024/May/036 Emissary Panda - Custom Tool SysUpdate |  |  |  |
|  | Adv/2024/May/037 Malicious IOCs |  |  |  |
|  | Adv/2024/May/038 Malicious IOCs |  |  |  |
|  | Adv/2024/May/039 Phishing Attack |  |  |  |