**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** |
|  | CMTX-I-055042024 Mythic Malware - APT36 campaign |  |  |  |
|  | CMTX-P042024285 Supershell Malware |  |  |  |
|  | CMTX-P042024295 Multiple Security Flaws in Judge Zero |  |  |  |
|  | CMTX-P-042024345 Raccoon Stealer |  |  |  |
|  | CMTX-P-042024325 SocGholish malware |  |  |  |
|  | CMTX-P-042024375 Amadey Malware Alert |  |  |  |
|  | CMTX-P-042024365 Emotet Malware |  |  |  |
|  | CMTX-P-042024385 Agent Tesla Malware Alert |  |  |  |
|  | CMTX-P-042024335 Redline malware |  |  |  |
|  | CMTX-P-042024355 Qbot Malware |  |  |  |
|  | CMTX-P-042024315 Trickbot malware |  |  |  |
|  | CMTX-P-042024305 Ursnif malware |  |  |  |
|  | CMTX-I-144042024 QuestRAT Malware - APT36 campaign |  |  |  |
|  | CMTX-I-025052024 Malicious Domains - Spear-Phishing & Malware Hosting Campaign |  |  |  |
|  | CMTX-P052024015 VacBan Stealer |  |  |  |
|  | CMTX-P052024975 PLUGX RAT ALERT 114 |  |  |  |
|  | CMTX-P052024024 IOCs related to Chinese Threat Actor Campaign |  |  |  |
|  | CMTX-P052024656 GH0ST RAT Malware |  |  |  |
|  | CMTX-P052024985 PLUGX RAT ALERT 115 |  |  |  |
|  | CMTX-P052024666 NJRAT Malware |  |  |  |
|  | CMTX-P052024676 QuasarRAT Malware ALERT 50 |  |  |  |
|  | CMTX-I-053052024 CrimsonRAT - APT36 campaign |  |  |  |
|  | CMTX-P052024945 SHADOWPAD Malware |  |  |  |
|  | CMTX-P052024995 PLUGX RAT ALERT 116 |  |  |  |
|  | CMTX-I-8080052024 Malicious Domains - Spear-Phishing & Malware Hosting Campaign |  |  |  |
|  | CMTX-P052024018 REDLINE STEALER MALWARE |  |  |  |
|  | CMTX-P052024025 ArcaneDoor Activity |  |  |  |
|  | CMTX-P052024028 RACCOON MALWARE |  |  |  |
|  | CMTX-I-445052024 Android RAT - APT36 Campaign |  |  |  |
|  | CMTX-P052024045 Two Critical Vulnerabilities (CVE-2024-21793 & CVE-2024-26026) Affecting F5 Next Central Manager |  |  |  |
|  | CMTX-P052024035 Active Exploitation of a critical vulnerability (CVE-2023-40000) Affecting LiteSpeed Cache plugin for WordPress |  |  |  |
|  | CMTX-P052024955 SHADOWPAD Malware |  |  |  |
|  | CMTX-P052024105 PLUGX RAT ALERT 117 |  |  |  |
|  | CMTX-I-021052024 Android RAT - IOCs |  |  |  |
|  | CMTX-P-052024055 Black Basta Ransomware |  |  |  |
|  | CMTX-I-636052024 Malicious Domains - Spear-Phishing Campaign |  |  |  |
|  | CMTX-P052024038 Agent Tesla Malware Alert |  |  |  |
|  | CMTX-P052024058 Emotet Malware |  |  |  |
|  | CMTX-P052024078 RACCOON MALWARE |  |  |  |
|  | CMTX-P052024088 Redline malware |  |  |  |
|  | CMTX-P052024118 Ursnif malware |  |  |  |
|  | CMTX-P052024108 Trickbot malware Alert |  |  |  |
|  | CMTX-P052024068 Qbot Malware |  |  |  |
|  | CMTX-P052024048 Amadey Malware Alert |  |  |  |
|  | CMTX-P052024098 SocGholish malware |  |  |  |
|  | CMTX-P052024686 QuasarRAT Malware ALERT 51 |  |  |  |
|  | CMTX-I-200052024 Mythic Malware - APT36 campaign |  |  |  |
|  | CMTX-I-404052024 SideCopy - C&C of Malware Campaign |  |  |  |
|  | CMTX-I-587052024 Malicious Domains - Spear-Phishings |  |  |  |
|  | CMTX-I-333052024 APT36 campaign |  |  |  |
|  | CMTX-I-400052024 Pakistan Based Malware Campaign |  |  |  |
|  | CMTX-P052024965 SHADOWPAD Malware |  |  |  |
|  | CMTX-P052024058 Emotet Malware |  |  |  |
|  | CMTX-P052024205 PLUGX RAT ALERT 118 |  |  |  |
|  | CMTX-P052024696 QuasarRAT Malware ALERT 52 |  |  |  |
|  | CMTX-I-409052024 AllaKore RAT - APT36 campaign |  |  |  |
|  | CMTX-P052024706 GH0ST RAT Malware |  |  |  |
|  | CMTX-P052024128 REDLINE STEALER MALWARE |  |  |  |
|  | CMTX-P052024138 RACCOON MALWARE |  |  |  |
|  | CMTX-I-304052024 Malicious Domains - Spear-Phishing |  |  |  |
|  | CMTX-P052024065 BlackTech Actor Activity |  |  |  |
|  | CMTX-P052024075 Zero Day Vulnerability in QNAP QTS |  |  |  |
|  | 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 |  |  |  |