**Cyber Security Advisories**

**Date: 30 September 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-092024085 MYTHIC/POSEIDON MALWARE CAMPAIGN |  |  |  |
|  | CMTX-P-092024095 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-092024105 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-876092024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P092024674 Command Injection Vulnerability Affecting Ivanti Cloud Service Appliance (CVE-2024-8190) |  |  |  |
|  | CMTX-P-092024115 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-950092024 C2 IP of Malware Targeting Govt. Officials |  |  |  |
|  | CMTX-P-092024125 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-007092024 Mythic Malware- APT36 campaign |  |  |  |
|  | CMTX-I-940092024 Malicious Domain used by Threat Actors |  |  |  |
|  | CMTX-P-092024135 PlugX Malware Campaign |  |  |  |
|  | CMTX-P092024944 New Variant of RansomHub Ransomware |  |  |  |
|  | CMTX-P-092024145 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-092024155 PlugX Malware Campaign |  |  |  |
|  | CMTX-P092024954 Relay server Nodes used by Chinese actors |  |  |  |
|  | CMTX-I-366092024 CrimsonRAT- APT36 campaign |  |  |  |
|  | CMTX-P092024964 Relay server Nodes used by Chinese actors |  |  |  |
|  | CMTX-I-521092024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-388092024 Android RAT Latest C&C IP |  |  |  |
|  | CMTX-I-901092024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P092024964 Interactsh  Tool |  |  |  |
|  | CMTX-I-884092024 Mythic Malware- APT36 campaign |  |  |  |
|  | CMTX-I-014092024 Malware Campaign Exfiltrating Data via Google API |  |  |  |
|  | CMTX-I-333092024 CrimsonRAT- APT36 campaign |  |  |  |
|  | CMTX-I-452092024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P092024974 EDR Disable tool used by Threat actors |  |  |  |
|  | CMTX-P092024984 Relay server Nodes used by Chinese actors |  |  |  |
|  | CMTX-P-092024175 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-092024165 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-7040920249 Agent Tesla Malware Alert |  |  |  |