**Cyber Security Advisories**

**Date: 17 October 2024**

**Name of Control Centre:**

| **S No** | **Vulnerability Note No** | **Applicable to Organisation** | **If Yes: Action Taken:** | **Remarks** |
| --- | --- | --- | --- | --- |
| **(Yes/No)** | **Yes / No/ Deferred** |
|  | CMTX-P102024075 Salt Typhoon Activity |  |  |  |
|  | CMTX-I-401102024 Mythic Malware- APT36 campaign |  |  |  |
|  | CMTX-I-400102024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P102024106 Blackout Ransomware |  |  |  |
|  | CMTX-P102024024 INC Ransomware |  |  |  |
|  | CMTX-P-102024034 Dark Crystal RAT (DC RAT) |  |  |  |
|  | CMTX-P102024044 Relay server Nodes used by Chinese actors |  |  |  |
|  | CMTX-P-102024174 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-102024164 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-500102024 Mythic Malware- APT36 campaign |  |  |  |
|  | CMTX-I-502102024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P102024054 Relay server Nodes used by Chinese actors |  |  |  |
|  | CMTX-P-102024064 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-102024074 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-102024084 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-301102024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-302102024 CrimsonRAT- APT36 campaign |  |  |  |
|  | CMTX-I-053102024 Mythic Malware- APT36 campaign |  |  |  |
|  | CMTX-I-053102024\_1 Mythic Malware- APT36 campaign |  |  |  |
|  | CMTX-P-102024034 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-587102024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P-502102024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-137102024 SideCopy Malware C&C Domain |  |  |  |
|  | CMTX-P102024094 Relay server Nodes used by Chinese actors |  |  |  |
|  | CMTX-P102024104 RCRU64 Ransomware |  |  |  |
|  | CMTX-I-025102024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-021102024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P-102024015 Critical Alert: MYTHIC Malware Campaign |  |  |  |
|  | CMTX-I-069102024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P102024114 Relay server Nodes used by Chinese actors |  |  |  |
|  | CMTX-P-102024124 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-102024134 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-080102024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-102024025 ACTIVE EXPLOITATION OF VEEAM VULNERABILITY (CVE-2024-40711) TO DEPLOY AKIRA AND FOG RANSOMWARE |  |  |  |
|  | CMTX-I-808102024 Recent IOCs of Chinese Malware Campaign |  |  |  |
|  | CMTX-102024025 ACTIVE EXPLOITATION OF VEEAM VULNERABILITY (CVE-2024-40711) TO DEPLOY AKIRA AND FOG RANSOMWARE |  |  |  |
|  | CMTX-P102024035 ACTIVE EXPLOITATION OF IVANTI CLOUD SERVICE APPLIANCE(CSA)FLAWS BY NATION STATE ADVERSARY |  |  |  |
|  | CMTX-I-443102024 SideCopy Malware C&C IP |  |  |  |
|  | CMTX-I-665102024 Malicious Domains used for Phishing |  |  |  |
|  | CMTX-I-389102024 Malicious Domains used by Threat Actors |  |  |  |