**Cyber Security Advisories**

**Date: 31 July 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-946072024 APT36 campaign |  |  |  |
|  | CMTX-I-952072024 Malicious Domains used by APT Threat Actors |  |  |  |
|  | CMTX-I-954072024 Suspicious Domain Spoofing CSC domain name |  |  |  |
|  | CMTX-P072024796 Atlantida Stealer |  |  |  |
|  | CMTX-P0720240508 BugSleep Malware |  |  |  |
|  | CMTX-I-956072024 APT36 - IOCs of Malware Campaign |  |  |  |
|  | CMTX-P072024816 QuasarRAT Malware ALERT 59 |  |  |  |
|  | CMTX-P072024806 APT17 THREAT GROUP ACTIVITY |  |  |  |
|  | CMTX-P0720240608 Beavertail Malware |  |  |  |
|  | CMTX-P072024826 QuasarRAT Malware ALERT 60 |  |  |  |
|  | CMTX-P072024836 Oneshell tool |  |  |  |
|  | CMTX-P072024135 Qilin Ransomware |  |  |  |
|  | CMTX-P072024145 TRINITY Ransomware |  |  |  |
|  | CMTX-I-875072024 SpyNote -  APT36 Campaign |  |  |  |
|  | CMTX-I-892072024 AsyncRAT - APT36 campaign |  |  |  |
|  | CMTX-P072024108 Prolific RAT |  |  |  |
|  | CMTX-P072024098 Lumma Stealer |  |  |  |
|  | CMTX-P072024114 TrollAgent Stealer |  |  |  |
|  | CMTX-P-5460720249 Agent Tesla Malware Alert |  |  |  |
|  | CMTX-P-2770720249 Redline Malware Alert |  |  |  |
|  | CMTX-P-4650720249 Emotet Malware Alert |  |  |  |
|  | CMTX-P-3410720249 Raccoon Malware Alert |  |  |  |
|  | CMTX-P-1890720249 SocGholish Malware Alert |  |  |  |
|  | CMTX-P-5830720249 Amadey Malware Alert |  |  |  |
|  | CMTX-P-8200720249 Qbot Malware Alert |  |  |  |
|  | CMTX-P-2490720249 Trickbot Malware Alert |  |  |  |
|  | CMTX-P-9250720249 Ursnif Malware Alert |  |  |  |
|  | CMTX-I-138072024 Malicious Domains used by Pakistan based Threat Actors |  |  |  |
|  | CMTX-I-432072024 Ahmyth Android Trojan |  |  |  |
|  | CMTX-P072024155 CUTTLEFISH MALWARE |  |  |  |
|  | CMTX-P072024124 TAG-109 Threat actor |  |  |  |
|  | CMTX-P072024846 SparkRAT Malware |  |  |  |
|  | CMTX-P072024118 BITRAT |  |  |  |
|  | CMTX-P072024134 APT45 Threat actor |  |  |  |
|  | CMTX-I-911072024 Malicious Domains used by Pakistan based Threat Actors |  |  |  |
|  | CMTX-P072024522 Threat actors exploit recent CrowdStrike update issue |  |  |  |
|  | CMTX-P072024165 LOSTINFO RANSOMWARE |  |  |  |
|  | CMTX-P072024856 Play Ransomware |  |  |  |
|  | CMTX-P-9110720249 Mirai Botnet Campaign |  |  |  |
|  | CMTX-P072024175 RA WORLD RANSOMWARE |  |  |  |
|  | CMTX-P072024144 Daggerfly threat Actor Activity |  |  |  |
|  | CMTX-I-170072024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-590072024 Malicious Domains used by Pakistan based Threat Actors |  |  |  |
|  | CMTX-I-765072024 Mythic Malware IOCs |  |  |  |
|  | CMTX-P072024605 SHADOWPAD Malware |  |  |  |
|  | CMTX-P072024065 PLUGX RAT ALERT 126 |  |  |  |
|  | CMTX-I-680072024 Malicious IP Hosting Malware |  |  |  |
|  | CMTX-P072024866 Stargazer Goblin recent activity |  |  |  |
|  | CMTX-P072024185 Rhysida Ransomware |  |  |  |
|  | CMTX-I-634072024 Malicious IP Hosting Malware |  |  |  |
|  | CMTX-P072024128 Blacksuit Ransomware (Rebrand of Royal Ransomware) |  |  |  |
|  | CMTX-P072024876 RansomHub Ransomware |  |  |  |
|  | CMTX-I-400072024 Mythic Malware- APT36 campaign |  |  |  |
|  | CMTX-P072024886 QuasarRAT Malware ALERT 61 |  |  |  |
|  | CMTX-I-500072024 Mythic Malware- APT36 campaign |  |  |  |
|  | CMTX-I-401072024 Malicious Domains used by Pakistan based Threat Actors |  |  |  |
|  | CMTX-I-501072024 Suspicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P072024874 IOCs related to Cobalt strike Malware |  |  |  |
|  | CMTX-P072024964 Critical vulnerability (CVE-2024-37085) in ESXi hypervisors |  |  |  |
|  | CMTX-P072024896 Mirai Botnet Campaign |  |  |  |
|  | CMTX-I-323072024 SideCopy - IOCs of Malware Campaign |  |  |  |
|  | CMTX-I-325072024 Recent IOCs of Malware Campaign |  |  |  |
|  | CMTX-I-335072024 CrimsonRAT - APT36 campaign |  |  |  |
|  | CMTX-I-901072024 CrimsonRAT- APT36 campaign |  |  |  |
|  | CMTX-I-345072024 Suspicious Domains used by Threat Actors |  |  |  |
|  | Adv/2024/Jul/038 CRITICAL VULNERABILITIES IN OPENSSH |  |  |  |
|  | Adv/2024/Jul/039 APT40 |  |  |  |
|  | Adv/2024/Jul/040 Active Exploitation of Critical Vulnerability (CVE-2024-4577) |  |  |  |
|  | Adv/2024/Jul/042 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | Adv/2024/Jul/043 Microsoft Windows Error “Blue Screen of Death (BSOD)” |  |  |  |
|  | Adv/2024/Jul/044 CoralRaider |  |  |  |
|  | Adv/2024/Jul/045 JRat Malware |  |  |  |
|  | Adv/2024/Jul/046 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | Adv/2024/Jul/047 Racoon Malware |  |  |  |
|  | Adv/2024/Jul/048 Malicious IOCs |  |  |  |
|  | Adv/2024/Jul/049 Trickbot malware |  |  |  |
|  | Adv/2024/Jul/050 Weekly Mirai Activity Report |  |  |  |