**Cyber Security Advisories**

**Date: 16 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-I-080092024 Malicious Domain used by Pakistan based Threat Actors |  |  |  |
|  | CMTX-P-3840920249 Agent Tesla Malware Alert |  |  |  |
|  | CMTX-P-8850920249 Raccoon Malware Alert |  |  |  |
|  | CMTX-P-7690920249 Amadey Malware Alert |  |  |  |
|  | CMTX-P-6350920249 Trickbot Malware Alert |  |  |  |
|  | CMTX-P-7980920249 Ursnif Malware Alert |  |  |  |
|  | CMTX-P-4400920249 Redline Malware Alert |  |  |  |
|  | CMTX-P-9850920249 SocGholish Malware Alert |  |  |  |
|  | CMTX-P-1940920249 Emotet Malware Alert |  |  |  |
|  | CMTX-P-5170920249 Qbot Malware Alert |  |  |  |
|  | CMTX-I-808092024 CrimsonRAT- APT36 campaign |  |  |  |
|  | CMTX-P092024025 SUPER JUMPER COVERT NETWORK |  |  |  |
|  | CMTX-I-053092024 Mythic Malware- APT36 campaign |  |  |  |
|  | CMTX-I-443092024 Phishing Campaign Targeting Credentials via Telegram API |  |  |  |
|  | CMTX-P092024986 ToneShell Malware Campaign |  |  |  |
|  | CMTX-I-445092024 Malicious Domain used by Pakistan based Threat Actors |  |  |  |
|  | CMTX-I-446092024 Phishing Campaign Targeting Credentials via Webex API |  |  |  |
|  | CMTX-P-092024035 KTLVdoor Malware |  |  |  |
|  | CMTX-P092024045 Cicada3301 Ransomware |  |  |  |
|  | CMTX-I-818092024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-023092024 Mythic Malware- APT36 campaign |  |  |  |
|  | CMTX-I-025092024 Mythic Malware- APT36 campaign |  |  |  |
|  | CMTX-P-092024045 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-092024055 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P092024996 Mallox Ransomware |  |  |  |
|  | CMTX-P092024106 BlackByte Ransomware |  |  |  |
|  | CMTX-I-020092024 Linux Malware C&C Domain and IP |  |  |  |
|  | CMTX-P092024065 ACTIVE EXPLOITATION OF GEOSERVER VULNERABILITY (CVE-2024-36401) |  |  |  |
|  | CMTX-I-022092024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-404092024 Malicious Domains Associated with Macro Embedded Documents |  |  |  |
|  | CMTX-I-500092024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-514082024 SideCopy Malware C&C IP |  |  |  |
|  | CMTX-P092024075 EARTH PRETA CAMPAIGN |  |  |  |
|  | CMTX-P092024116 EchoStrike tool |  |  |  |
|  | CMTX-092024085 Akira Ransomware Gang Exploiting SonicWall Vulnerability |  |  |  |
|  | CMTX-P-1140920249 MacroPack-Generated Malicious Documents |  |  |  |
|  | CMTX-P-2140920249 Loki backdoor |  |  |  |
|  | CMTX-I-525092024 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-MAW-2024-08-30-28 Fabookie Infostealer |  |  |  |
|  | TA-MAW-2024-08-30-029 PG\_MEM  Malware |  |  |  |
|  | TA-RAN-2024-09-02-001 Ransom Hub Ransomware |  |  |  |
|  | TA-MAW-2024-09-03-001 Cheana Stealer |  |  |  |
|  | TA-MAW-2024-09-04-002 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-MAW-2024-09-04-003 Sedexp Malware |  |  |  |
|  | VA-2024-09-04-001 ACTIVE EXPLOITATION OF PUBLIC FACING APPLICATION VULNERABILITIES |  |  |  |
|  | TA-MAW-2024-09-04-004 Malicious IPs Targeting Critical Sectors |  |  |  |
|  | TA-MAW-2024-09-05-005 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-MAW-2024-09-05-006 ToneShell Malware Campaign |  |  |  |
|  | VA-2024-09-06-002 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-PHI-2024-09-06-01 Phishing Domains |  |  |  |
|  | TA-MAW-2024-09-06-007 Malicious IOCs |  |  |  |
|  | TA-PHI-2024-09-13-02 Phishing Attack |  |  |  |
|  | TA-PHI-2024-09-13-03 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-APT-2024-09-13-001 Mythic Malware- APT36 Campaign |  |  |  |
|  | TA-RAN-2024-09-13-002 Cicada3301 Ransomware |  |  |  |
|  | TA-MAW-2024-09-13-008 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-PHI-2024-09-13-004 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-APT-2024-09-13-002 SideCopy Malware C&C IP |  |  |  |
|  | TA-RAN-2024-09-13-003 BlackByte Ransomware |  |  |  |
|  | TA-MAW-2024-09-13-009 Linux Malware C&C Domain and IP |  |  |  |