**Cyber Security Advisories**

**Date: 31 December 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-122024874 IOAs of suspicious domains |  |  |  |
|  | CMTX-I-563122024 DDNS Domains Targeting Government Organizations |  |  |  |
|  | CMTX-I-389122024 SpyNote-  APT36 Campaign |  |  |  |
|  | CMTX-I-389124874 AllaKore RAT Malware |  |  |  |
|  | CMTX-P-122024724 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-122024714 PlugX Malware Campaign |  |  |  |
|  | CMTX-P122024545 Active Exploitation of a Critical Flaw |  |  |  |
|  | CMTX-I-309124874 IOCs of China-based Malware Campaign |  |  |  |
|  | CMTX-I-626124874 IOAs of suspicious domains |  |  |  |
|  | CMTX-P-VUL-1220243314 Prominent Vulnerability List |  |  |  |
|  | CMTX-P-122024734 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-122024248 HiatusRAT Targeting IoT Devices |  |  |  |
|  | CMTX-P-122024258 Advisory on  Ransomware As a Service continuous  exploitation of "Bring Your Own Vulnerable Driver" (BYOVD) Techniques for Defense Evasion |  |  |  |
|  | CMTX-P-122024744 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-122024754 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-670124874 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-954122024 CrimsonRAT- APT36 campaign |  |  |  |
|  | CMTX-I-511122024 Mythic Malware- Pakistan Based Malware Campaign |  |  |  |
|  | CMTX-I-338122024 Malware Targeting Government Officials via Spear-Phishing |  |  |  |
|  | CMTX-P-122024764 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-I-512122024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-256122024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P-122024804 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-122024794 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-122024844 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-122024824 PlugX Malware Campaign |  |  |  |
|  | TA-APT-2024-12-17-004 CrimsonRAT- APT36 campaign |  |  |  |
|  | TA-PHI-2024-12-17-006 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-PHI-2024-12-17-007 DDNS Domains Targeting Government Organizations |  |  |  |
|  | TA-MAW-2024-12-17-009 PHPsert Web shell |  |  |  |
|  | VA-2024-12-17-005 Prominent Vulnerability List |  |  |  |
|  | VA-2024-12-17-006 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-MAW-2024-12-18-010 Weekly Mirai Activity Report |  |  |  |
|  | TA-MAW-2024-12-18-011 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-MAW-2024-12-20-012 AllaKore RAT Malware |  |  |  |
|  | TA-APT-2024-12-20-004 SpyNote- APT36 Campaign |  |  |  |
|  | VA-2024-12-20-007 Active Exploitation of a Critical Flaw (CVE-2024-53677) Affecting Apache Struts |  |  |  |
|  | TA-MAW-2024-12-20-013 IOCs of Malware Campaign |  |  |  |
|  | TA-MAW-2024-12-23-014 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | VA-2024-12-23-008 Prominent Vulnerability List |  |  |  |
|  | TA-PHI-2024-12-23-008  Malicious Domains used by Threat Actors |  |  |  |
|  | VA-2024-12-23-009 Password-Spraying Attack |  |  |  |
|  | TA-RAN-2024-12-24-003 Increased RansomHub activity reveals new tools and TTPs |  |  |  |
|  | TA-MAW-2024-12-24-015 Weekly Mirai Activity Report |  |  |  |
|  | TA-MAW-2024-12-24-016 HiatusRAT Targeting IoT Devices (Web Cameras and DVRs) |  |  |  |
|  | TA-RAN-2024-12-26-004 Ransomware as a Service (RaaS) using "Bring Your Own Vulnerable Driver" (BYOVD) Techniques for Defense Evasion |  |  |  |
|  | TA-PHI-2024-12-26-008 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-PHI-2024-12-30-009 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-APT-2024-12-30-005 Mythic Malware- APT36 Campaign |  |  |  |