**Cyber Security Advisories**

**Date: 28 February 2025**

**Name of Control Centre:**

| **S No** | **Vulnerability Note No** | **Applicable to Organisation** | **If Yes: Action Taken:** | **Remarks** |
| --- | --- | --- | --- | --- |
| **(Yes/No)** | **Yes / No/ Deferred** |
|  | TA-MAW-2025-01-31-037 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-PHI-2025-01-31-018 Phishing Attack |  |  |  |
|  | TA-MAW-2025-01-31-038 Threat Actors Leverage WsgiDAV Infrastructure to Distribute Multiple RAT via Python-Based Malware Loader |  |  |  |
|  | TA-MAW-2025-01-31-039 Malicious IOCs |  |  |  |
|  | VA-2025-02-03-001 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-MAW-2025-02-03-001 CL-STA-0048 Campaign |  |  |  |
|  | TA-RAN-2025-02-03-001 Hellcat Ransomware |  |  |  |
|  | TA-PHI-2025-02-03-001 Phishing Attack |  |  |  |
|  | TA-PHI-2025-02-04-002 Phishing Attack |  |  |  |
|  | TA-MAW-2025-02-04-002 Weekly Mirai Activity Report |  |  |  |
|  | TA-MAW-2025-02-04-003 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-MAW-2025-02-04-004 AMOS Stealer |  |  |  |
|  | TA-PHI-2025-02-04-003 Phishing Attack |  |  |  |
|  | TA-PHI-2025-02-04-004 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-PHI-2025-02-04-005 Phishing Attack |  |  |  |
|  | TA-MAW-2025-02-06-005 Sliver Implant |  |  |  |
|  | TA-MAW-2025-02-06-006 Malicious IOCs |  |  |  |
|  | VA-2025-02-06-002 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-MAW-2025-02-06-007 OtterCookie Malware |  |  |  |
|  | TA-MAW-2025-02-06-008 Phorpiex - Downloader Delivering Ransomware |  |  |  |
|  | TA-MAW-2025-02-07-009 MEDIAARENA MALWARE |  |  |  |
|  | TA-RAN-2025-02-07-002 WINDOWS LOCKER RANSOMWARE |  |  |  |
|  | TA-APT-2025-02-07-001 CrimsonRAT-  APT36 Campaign |  |  |  |
|  | TA-PHI-2025-02-07-006  Malicious Domain Imitating Indian Navy Website and Hosting APK |  |  |  |
|  | VA-2025-02-07-003 Active Exploitation of Vulnerability (CVE-2025-22604) Affecting Cacti |  |  |  |
|  | TA-PHI-2025-02-10-007 Malicious Google Ads Used in Phishing Attack |  |  |  |
|  | TA-MI-2025-02-10-001 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-MAW-2025-02-10-010 Threat Actors Leverage WsgiDAV Infrastructure to Distribute Multiple RAT via Python-Based Malware Loader |  |  |  |
|  | TA-PHI-2025-02-10-008 Phishing Attack |  |  |  |
|  | TA-RAN-2025-02-10-003 Arcus Media Ransomware |  |  |  |
|  | VA-2025-02-10-004 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | VA-2025-02-11-005  Prominent Vulnerability List |  |  |  |
|  | TA-MAW-2025-02-11-011 Code Injection Attacks using publicly available ASP.NET machine keys |  |  |  |
|  | TA-APT-2025-02-11-002 CrimsonRAT-  APT36 Campaign |  |  |  |
|  | TA-MI-2025-02-11-002 Malicious IOCs |  |  |  |
|  | TA-MI-2025-02-13-003 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-MAW-2025-02-13-013 IOCs related to njRAT family |  |  |  |
|  | TA-PHI-2025-02-13-010 Phishing Attack |  |  |  |
|  | TA-RAN-2025-02-13-005 Presence of  AvosLocker Ransomware observed in Indian CyberSpace |  |  |  |
|  | TA-TAG-2025-02-13-002 Presence of Unknown Threat Actor in Indian CyberSpace |  |  |  |
|  | TA-RAN-2025-02-13-006 Presence of Unknown Ransomware Variant observed in Indian CyberSpace |  |  |  |
|  | TA-MAW-2025-02-13-014 QSC - A Multi-Plugin Framework |  |  |  |
|  | TA-PHI-2025-02-13-011 Phishing Attack |  |  |  |
|  | TA-TAG-2025-02-13-003 Threat Actor DragonRank |  |  |  |
|  | TA-TAG-2025-02-14-004 PurpleBravo Actor Activity |  |  |  |
|  | TA-PHI-2025-02-14-012 Malicious Domains used by Threat Actors |  |  |  |
|  | VA-2025-02-14-006 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-PHI-2025-02-17-013 Phishing Attack |  |  |  |
|  | TA-MI-2025-02-17-004 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-PHI-2025-02-17-014 Phishing Domains |  |  |  |
|  | TA-MI-2025-02-17-005 Malicious IOCs |  |  |  |
|  | TA-PHI-2025-02-19-016 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-MI-2025-02-19-006 Malicious IOCs |  |  |  |
|  | TA-MI-2025-02-19-007 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | VA-2025-02-19-009 CVE - KB Correlation, Feb 2025 |  |  |  |
|  | VA-2025-02-06-19-008 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-TAG-2025-02-19-005 Threat Actor Seashell Blizzard - BadPilot campaign |  |  |  |
|  | TA-MAW-2025-02-19-018 Keyplug Malware |  |  |  |
|  | TA-PHI-2025-02-21-018 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-TAG-2025-02-21-006 RevivalStone - a new attack campaign attributed to "Winnti Group" |  |  |  |
|  | TA-RAN-2025-02-21-008 Ghost (Cring) Ransomware |  |  |  |
|  | TA-MI-2025-02-21-008 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-PHI-2025-02-24-019 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-APT-2025-02-24-005 Mythic Malware- APT36 Campaign |  |  |  |
|  | TA-APT-2025-02-24-006 APT36 Campaign |  |  |  |
|  | TA-MAW-2025-02-25-019 Threat actors using Blockchain to Store Malicious Payloads |  |  |  |
|  | TA-TAG-2025-02-25-007 Threat Actor Stately Taurus |  |  |  |
|  | TA-MAW-2025-02-25-020 FINALDRAFT Malware |  |  |  |
|  | TA-MAW-2025-02-25-021 FERRET Malware |  |  |  |
|  | TA-MAW-2025-02-25-022 Weekly Mirai Activity Report |  |  |  |
|  | TA-PHI-2025-02-25-020 Malicious Domains used by Threat Actors |  |  |  |
|  | VA-2025-02-25-010  Prominent Vulnerability List |  |  |  |
|  | VA-2025-02-25-011 ACTIVE EXPLOITATION OF CVE-2024-24919 AFFECTING CHECK POINT NETWORK GATEWAY |  |  |  |
|  | TA-MI-2025-02-25-009 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-PHI-2025-02-27-021 Phishing Attack |  |  |  |
|  | VA-2025-02-27-012 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-PHI-2025-02-27-022 Phishing Domains |  |  |  |
|  | TA-TAG-2025-02-27-008 Threat Actor using ORB network |  |  |  |
|  | TA-PHI-2025-02-27-023 Malicious Domains used by Threat Actors |  |  |  |