**Cyber Security Advisories**

**Date: 16 August 2024**

**Name of Control Centre:**

| **S No** | **Vulnerability Note No** | **Applicable to Organisation** | **If Yes: Action Taken:** | **Remarks** |
| --- | --- | --- | --- | --- |
| **(Yes/No)** | **Yes / No/ Deferred** |
|  | Adv/2024/Jul/051 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | Adv/2024/Jul/052 Threat actors exploit recent CrowdStrike update issue |  |  |  |
|  | Adv/2024/Jul/053 Malicious IOCs |  |  |  |
|  | Adv/2024/Jul/054 CUTTLEFISH MALWARE |  |  |  |
|  | Adv/2024/Jul/055 Mirai Botnet Campaign |  |  |  |
|  | Adv/2024/Jul/056 RA WORLD RANSOMWARE |  |  |  |
|  | Adv/2024/Jul/057 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | Adv/2024/Jul/058 Bitrat Backdoor |  |  |  |
|  | Adv/2024/Aug/002 Critical Vulnerability (CVE-2024-37085) in VMware ESXi hypervisors |  |  |  |
|  | Adv/2024/Aug/003 Phishing Attack |  |  |  |
|  | Adv/2024/Aug/005 Update on Ransomware attacks on C-Edge Technologies |  |  |  |
|  | Adv/2024/Aug/004 Malicious IP Targeting Critical Sectors |  |  |  |
|  | Adv/2024/Aug/006 Phishing Attacks |  |  |  |
|  | Adv/2024/Aug/007 Lynx Ransomware |  |  |  |
|  | Adv/2024/Aug/008 Covenant C2 |  |  |  |
|  | Adv/2024/Aug/009 RedLima (APT15) Threat Actor Campaign |  |  |  |
|  | Adv/2024/Aug/010 Cobalt Strike Malware |  |  |  |
|  | Adv/2024/Aug/013 Atlantida Stealer |  |  |  |
|  | Adv/2024/Aug/015 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | Adv/2024/Aug/011 Beavertail Malware |  |  |  |
|  | Adv/2024/Aug/012 BugSleep Malware |  |  |  |
|  | Adv/2024/Aug/014 Oneshell tool |  |  |  |
|  | Adv/2024/Aug/016 QuasarRAT Malware |  |  |  |
|  | Adv/2024/Aug/017 Lumma Stealer |  |  |  |
|  | Adv/2024/Aug/018 Prolific RAT |  |  |  |
|  | Adv/2024/Aug/019 Qbot Malware |  |  |  |
|  | Adv/2024/Aug/020 Racoon Malware |  |  |  |
|  | Adv/2024/Aug/021 Redline Malware |  |  |  |
|  | Adv/2024/Aug/022 TRINITY Ransomware |  |  |  |
|  | Adv/2024/Aug/023 Qilin Ransomware |  |  |  |
|  | Adv/2024/Aug/024 Emotet Malware |  |  |  |
|  | Adv/2024/Aug/027 SocGholish Malware |  |  |  |
|  | Adv/2024/Aug/029 Threat Actor TAG-109 |  |  |  |
|  | Adv/2024/Aug/028 Trickbot Malware |  |  |  |
|  | Adv/2024/Aug/030 Play Ransomware |  |  |  |
|  | Adv/2024/Aug/025 Ursnif Malware |  |  |  |
|  | Adv/2024/Aug/026 Amadey Malware |  |  |  |
|  | Adv/2024/Aug/031 Transparent Tribe AKA APT36 |  |  |  |
|  | Adv/2024/Aug/032 Malicious IP Targeting Critical Sectors |  |  |  |
|  | Adv/2024/Aug/033 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | Adv/2024/Aug/034 Threat Actor Daggerfly |  |  |  |
|  | TA-RAN-2024-08-12-001 BlackSuit Ransomware |  |  |  |
|  | TA-RAN-2024-08-12-002 Rhysida Ransomware |  |  |  |
|  | TA-RAN-2024-08-12-003 HorrorDead Ransomware |  |  |  |
|  | VA-2024-08-12-001 Vulnerabilities in OpenVPN |  |  |  |
|  | TA-MAW-2024-08-12-001 Stargazer Goblin recent activity |  |  |  |
|  | SA-2024-08-12-001 Cyber Security Alert for Independence Day |  |  |  |
|  | VA-2024-08-13-002 Microsoft Office Spoofing Vulnerability |  |  |  |
|  | TA-MAW-2024-08-13-003 REDLINE STEALER Malware |  |  |  |
|  | TA-MAW-2024-08-14-004 Mirai Malware |  |  |  |
|  | TA-MAW-2024-08-14-005 Arc Silt Malware |  |  |  |
|  | TA-MAW-2024-08-13-002 Info Stealer Malware Campaign |  |  |  |
|  | TA-RAN-2024-08-14-005 AzzaSec Ransomware |  |  |  |
|  | TA-MAW-2024-08-14-006 Agent Tesla Malware |  |  |  |
|  | TA-RAN-2024-08-14-007 Mimic Ransomware |  |  |  |
|  | TA-RAN-2024-08-14-006 Cronus Ransomware |  |  |  |
|  | TA-MAW-2024-08-14-008 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-APT-2024-08-14-001 APT41 Threat Actor Campaign |  |  |  |
|  | TA-RAN-2024-08-14-008 Blacksuit Ransomware |  |  |  |
|  | TA-MAW-2024-08-14-009 Weekly Mirai Activity Report |  |  |  |
|  | VA-2024-08-14-003 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-TAG-2024-08-14-001 Increase in Hacktivist Campaign activity |  |  |  |