**Cyber Security Advisories**

**Date: 30 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-P-092024085 MYTHIC/POSEIDON MALWARE CAMPAIGN |  |  |  |
|  | CMTX-P-092024095 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-092024105 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-876092024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P092024674 Command Injection Vulnerability Affecting Ivanti Cloud Service Appliance (CVE-2024-8190) |  |  |  |
|  | CMTX-P-092024115 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-950092024 C2 IP of Malware Targeting Govt. Officials |  |  |  |
|  | CMTX-P-092024125 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-007092024 Mythic Malware- APT36 campaign |  |  |  |
|  | CMTX-I-940092024 Malicious Domain used by Threat Actors |  |  |  |
|  | CMTX-P-092024135 PlugX Malware Campaign |  |  |  |
|  | CMTX-P092024944 New Variant of RansomHub Ransomware |  |  |  |
|  | CMTX-P-092024145 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-092024155 PlugX Malware Campaign |  |  |  |
|  | CMTX-P092024954 Relay server Nodes used by Chinese actors |  |  |  |
|  | CMTX-I-366092024 CrimsonRAT- APT36 campaign |  |  |  |
|  | CMTX-P092024964 Relay server Nodes used by Chinese actors |  |  |  |
|  | CMTX-I-521092024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-388092024 Android RAT Latest C&C IP |  |  |  |
|  | CMTX-I-901092024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P092024964 Interactsh  Tool |  |  |  |
|  | CMTX-I-884092024 Mythic Malware- APT36 campaign |  |  |  |
|  | CMTX-I-014092024 Malware Campaign Exfiltrating Data via Google API |  |  |  |
|  | CMTX-I-333092024 CrimsonRAT- APT36 campaign |  |  |  |
|  | CMTX-I-452092024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P092024974 EDR Disable tool used by Threat actors |  |  |  |
|  | CMTX-P092024984 Relay server Nodes used by Chinese actors |  |  |  |
|  | CMTX-P-092024175 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-092024165 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-7040920249 Agent Tesla Malware Alert |  |  |  |
|  | TA-PHI-2024-09-17-05 Phishing Attack |  |  |  |
|  | TA-MAW-2024-09-17-010 MacroPack-Generated Malicious Documents |  |  |  |
|  | TA-MAW-2024-09-17-011 Malicious Domains Associated with Macro Embedded Documents |  |  |  |
|  | TA-RAN-2024-09-17-004 Mallox Ransomware |  |  |  |
|  | TA-MAW-2024-09-17-012 Poseidon Malware |  |  |  |
|  | TA-RAN-2024-09-17-005 Akira Ransomware Gang Exploiting SonicWall Vulnerability |  |  |  |
|  | TA-PHI-2024-09-18-006 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-MAW-2024-09-18-013 EchoStrike tool |  |  |  |
|  | TA-MAW-2024-09-18-0014 Weekly Mirai Activity Report |  |  |  |
|  | VA-2024-09-19-003 ACTIVE EXPLOITATION OF GEOSERVER VULNERABILITY (CVE-2024-36401) |  |  |  |
|  | TA-APT-2024-09-19-004 Mythic Malware- APT36 Campaign |  |  |  |
|  | TA-APT-2024-09-19-003 EARTH PRETA CAMPAIGN |  |  |  |
|  | TA-MAW-2024-09-20-015 Loki Backdoor |  |  |  |
|  | TA-MAW-2024-09-20-016 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-PHI-2024-09-20-007 Phishing Attack |  |  |  |
|  | TA-APT-2024-09-20-005 Advanced Persistent Threat Actors targeting Critical Sectors |  |  |  |
|  | VA-2024-09-20-005 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-MAW-2024-09-20-017 C2 IP of Malware Targeting Govt. Officials |  |  |  |
|  | TA-MAW-2024-09-20-018 Malicious IOCs |  |  |  |
|  | TA-APT-2024-09-20-006 Mythic Malware- APT36 Campaign |  |  |  |
|  | TA-PHI-2024-09-20-008 Phishing Domains |  |  |  |
|  | VA-2024-09-20-004 hreat Actors Exploiting Command Injection Vulnerability in Ivanti Cloud Service Appliance |  |  |  |
|  | TA-TAG-2024-09-23-001 Threat Actors RedJuliett |  |  |  |
|  | TA-RAN-2024-09-23-006 RansomHub Ransomware |  |  |  |
|  | TA-APT-2024-09-24-007 APT 36 using CrimsonRAT Malware |  |  |  |
|  | TA-RAN-2024-09-24-009  Phishing Attack |  |  |  |
|  | TA-PHI-2024-09-24-010 Phishing Attack |  |  |  |
|  | TA-MAW-2024-09-24-020 Android RAT Latest C&C IP |  |  |  |
|  | TA-PHI-2024-09-24-011 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-MAW-2024-09-24-019 IOCs related to Various Malware |  |  |  |
|  | TA-MAW-2024-09-24-021 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-APT-2024-09-25-008 Mythic Malware- APT36 Campaign |  |  |  |
|  | VA-2024-09-25-006 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-PHI-2024-09-24-012 Phishing Attack |  |  |  |
|  | TA-APT-2024-09-27-009 APT 36 using CrimsonRAT Malware |  |  |  |
|  | TA-MAW-2024-09-27-022 Malware Campaign Exfiltrating Data via Google API |  |  |  |
|  | TA-MAW-2024-09-27-024 Interactsh Tool |  |  |  |
|  | TA-MAW-2024-09-27-023 Threat actors leveraging HRSword to disable EDR Defenses |  |  |  |
|  | TA-MAW-2024-09-27-026 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-PHI-2024-09-27-013 Malicious Domains used by Threat Actors |  |  |  |