**Cyber Security Advisories**

**Date: 16 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-P112024905 CHINESE BASED THREAT ACTOR (APT 19) ACTIVITY (TLP:CLEAR) |  |  |  |
|  | CMTX-I-080122024 CrimsonRAT- APT36 campaign [TLP: AMBER] |  |  |  |
|  | CMTX-P-122024814 Cumulative Suspicious Domains--ALERT5, TLP-RED |  |  |  |
|  | CMTX-P-122024014 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-122024055 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-122024065 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-808122024 Pakistan Based Malware Campaign |  |  |  |
|  | CMTX-I-655122024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-443122024 CrimsonRAT- APT36 campaign |  |  |  |
|  | CMTX-P-122024824 Cumulative Suspicious Domains |  |  |  |
|  | CMTX-P-122024834 Cumulative Suspicious Domains |  |  |  |
|  | CMTX-P-122024844 Cumulative Suspicious Domains |  |  |  |
|  | CMTX-P-VUL-1220243315 Prominent Vulnerability List |  |  |  |
|  | CMTX-P-122024105 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-122024205 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-I-554122024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P122024704 Guptiminer Malware |  |  |  |
|  | CMTX-I-633122024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P-122024775 DOGCALL MALWARE |  |  |  |
|  | CMTX-I-588122024 Threat Actors Using Legitimate Web Services/APIs for Data Exfiltration |  |  |  |
|  | CMTX-I-328122024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P-122024885 Exfiltration Risk from PowerSCP Stealer |  |  |  |
|  | CMTX-P122024995 Active Exploitation of a Critical Flaw (CVE-2024-50623) Affecting CLEO's File Transfer Products |  |  |  |
|  | CMTX-I-890122024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-122024871 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P-VUL-1220240015 Prominent Vulnerability List |  |  |  |
|  | CMTX-P-122024854 Cumulative Suspicious Domains |  |  |  |
|  | CMTX-P-122024905  SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-122024915 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-020122024 CrimsonRAT- APT36 campaign |  |  |  |
|  | CMTX-I-007122024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P-122024178 Relay server Nodes used by Chinese actors |  |  |  |
|  | CMTX-P-122024935 PHPsert Web shell |  |  |  |
|  | CMTX-I-122024874 IOAs of suspicious domains |  |  |  |
|  | TA-PHI-2024-12-04-001 Phishing Attack |  |  |  |
|  | TA-APT-2024-12-04-002 APT 19 |  |  |  |
|  | TA-APT-2024-12-04-001 CrimsonRAT- APT36 campaign |  |  |  |
|  | TA-MAW-2024-12-04-001 Weekly Mirai Activity Report |  |  |  |
|  | VA-2024-12-05-001 CVE - KB Correlation |  |  |  |
|  | TA-MAW-2024-12-06-002 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-TAG-2024-12-06-001 State-Sponsored Threat Actor's Cyber-Espionage Campaigns |  |  |  |
|  | TA-APT-2024-12-06-003 CrimsonRAT- APT36 campaign |  |  |  |
|  | TA-PHI-2024-12-06-002 Malicious Domains used by Threat Actors |  |  |  |
|  | VA-2024-12-06-002 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | TA-RAN-2024-12-10-001 Ransomware Attack by Executing HRSword Tool |  |  |  |
|  | TA-PHI-2024-12-10-003 Phishing Attack |  |  |  |
|  | TA-MAW-2024-12-10-003 Malicious IOCs |  |  |  |
|  | TA-MAW-2024-12-11-004 Weekly Mirai Activity Report |  |  |  |
|  | TA-PHI-2024-12-11-004 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-RAN-2024-12-11-002 Ransomware Attack by Executing HRSword Tool |  |  |  |
|  | TA-MAW-2024-12-11-006 DOGCALL MALWARE |  |  |  |
|  | TA-MAW-2024-12-11-005 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-MAW-2024-12-12-007 Exfiltration Risk from PowerSCP Stealer |  |  |  |
|  | TA-MAW-2024-12-13-008 Threat Actors Using Legitimate Web Services/APIs for Data Exfiltration |  |  |  |
|  | TA-PHI-2024-12-13-005 Malicious Domains used by Threat Actors |  |  |  |
|  | VA-2024-12-13-004 Active Exploitation of a Critical Flaw (CVE-2024-50623) Affecting CLEO's File Transfer Products |  |  |  |