**Cyber Security Advisories**

**Date: 17 July 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-194062024 SpyNote -  APT36 Campaign |  |  |  |
|  | CMTX-I-020062024 CrimsonRAT - APT36 campaign |  |  |  |
|  | CMTX-P062024005 PLUGX RAT ALERT 123 |  |  |  |
|  | CMTX-P062024205 SHADOWPAD Malware |  |  |  |
|  | CMTX-I-021072024 Mythic Malware - APT36 campaign |  |  |  |
|  | CMTX-P072024015 Circulation of Phishing email contain links to counterfeit CERT-In websites |  |  |  |
|  | CMTX-I-025072024 Suspicious Domain Spoofing State Govt. Domain |  |  |  |
|  | CMTX-I-080072024 Malicious Domain Spoofing CERT-In's Domain |  |  |  |
|  | CMTX-I-808072024 Malicious Domains used by Pakistan based Threat Actors |  |  |  |
|  | CMTX-P072024025 RADNET64 Hacktivist Group |  |  |  |
|  | CMTX-P072024035 Suspicious domain related to threat actor |  |  |  |
|  | CMTX-P072024305 SHADOWPAD Malware |  |  |  |
|  | CMTX-I-022072024 Malicious Domains used by Pakistan based Threat Actors |  |  |  |
|  | CMTX-I-053072024 Mythic Malware - APT36 campaign |  |  |  |
|  | CMTX-I-0445072024 Malicious Domains used by Pakistan based Threat Actors |  |  |  |
|  | CMTX-P072024766 QuasarRAT Malware ALERT 57 |  |  |  |
|  | CMTX-P072024018 Redline malware |  |  |  |
|  | CMTX-P072024028 RACCOON MALWARE |  |  |  |
|  | CMTX-P072024015 PLUGX RAT ALERT 124 |  |  |  |
|  | CMTX-P072024405 SHADOWPAD Malware |  |  |  |
|  | CMTX-P072024045 IOCs Related to Chinese Threat Actor |  |  |  |
|  | CMTX-I-022072024 Malicious Domains used by Pakistan based Threat Actors |  |  |  |
|  | CMTX-I-0449072024 Malicious Domains used by Pakistan based Threat Actors |  |  |  |
|  | CMTX-I-587072024 IOCs of Poseidon Stealer Targeting MacOS |  |  |  |
|  | CMTX-I-007072024 Mythic Malware - Cumulative IOCs |  |  |  |
|  | CMTX-P072024055 APT-40 THREAT ACTOR GROUP |  |  |  |
|  | CMTX-P0720240408 Eldorado RANSOMWARE |  |  |  |
|  | CMTX-P072024505 SHADOWPAD Malware |  |  |  |
|  | CMTX-P072024065 SNEAKY CHEF THREAT ACTOR |  |  |  |
|  | CMTX-I-520072024 Malicious Domain |  |  |  |
|  | CMTX-P-3610720249 Amadey Malware Alert |  |  |  |
|  | CMTX-P-5210720249 Agent Tesla Malware Alert |  |  |  |
|  | CMTX-P-9710720249 Emotet Malware Alert |  |  |  |
|  | CMTX-P072024075 CRITICAL VULNERABILITIES IN OPENSSH |  |  |  |
|  | CMTX-P-8440720249 Qbot Malware Alert |  |  |  |
|  | CMTX-P-8450720249 Raccoon Malware Alert |  |  |  |
|  | CMTX-P-4660720249 SocGholish Malware Alert |  |  |  |
|  | CMTX-P-2370720249 Redline Malware Alert |  |  |  |
|  | CMTX-P-5940720249 Trickbot Malware Alert |  |  |  |
|  | CMTX-P-2500720249 Ursnif Malware Alert |  |  |  |
|  | CMTX-I-389072024 Malicious Domains used by Pakistan based Threat Actors |  |  |  |
|  | CMTX-I-993072024 Malicious Domains used by Pakistan based Threat Actors |  |  |  |
|  | CMTX-I-995072024 Malicious Domains used by Pakistan based Threat Actors |  |  |  |
|  | CMTX-P072024095 MYTHIC MALWARE |  |  |  |
|  | CMTX-P072024105 RipperSec Hacktivist Group |  |  |  |
|  | CMTX-P072024115 Atomic Stealer (AMOS Variant) |  |  |  |
|  | CMTX-P072024134 IOCs related to Chinese Threat Actor Campaign |  |  |  |
|  | CMTX-P072024555 SHADOWPAD Malware |  |  |  |
|  | CMTX-P072024055 PLUGX RAT ALERT 125 |  |  |  |
|  | CMTX-P072024125 Active Exploitation of a Critical Vulnerability (CVE-2024-4577) Affecting PHP |  |  |  |
|  | CMTX-I-932072024 SideCopy - IOCs of Malware Campaign |  |  |  |
|  | CMTX-P072024786 QuasarRAT Malware ALERT 58 |  |  |  |
|  | CMTX-I-942072024 Malicious Domain Spoofing CERT-In's Domain |  |  |  |
|  | Adv/2024/Jun/040 GH0ST RAT Malware |  |  |  |
|  | Adv/2024/Jun/041 Emotet Malware |  |  |  |
|  | Adv/2024/Jun/042 Qbot Malware |  |  |  |
|  | Adv/2024/Jun/043 QuasarRAT Malware |  |  |  |
|  | Adv/2024/Jun/044 Racoon Malware |  |  |  |
|  | Adv/2024/Jun/045 Weekly Mirai Activity Report |  |  |  |
|  | Adv/2024/Jul/001 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | Adv/2024/Jul/002 PlugX RAT Malware |  |  |  |
|  | Adv/2024/Jul/003 Phishing Attack |  |  |  |
|  | Adv/2024/Jul/004 Transparent Tribe AKA APT36 |  |  |  |
|  | Adv/2024/Jul/009 LOCKBIT Ransomware |  |  |  |
|  | Adv/2024/Jul/010 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | Adv/2024/Jul/011 ACTIVE EXPLOITATION OF CRITICAL VULNERABILITY (CVE-2024-28995) |  |  |  |
|  | Adv/2024/Jul/005 Amadey Malware |  |  |  |
|  | Adv/2024/Jul/006 Trickbot malware |  |  |  |
|  | Adv/2024/Jul/007 Ursnif malware |  |  |  |
|  | Adv/2024/Jul/008 SparkRAT  Malware |  |  |  |
|  | Adv/2024/Jul/012 Pantegana Malware |  |  |  |
|  | Adv/2024/Jul/013 SocGholish Malware |  |  |  |
|  | Adv/2024/Jul/014 RedLine Malware |  |  |  |
|  | Adv/2024/Jul/015 Phishing Attack |  |  |  |
|  | Adv/2024/Jul/016 Malicious IP in Indian Cyberspace |  |  |  |
|  | Adv/2024/Jul/017 Fickle Stealer |  |  |  |
|  | Adv/2024/Jul/018 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | Adv/2024/Jul/022 Weekly Mirai Activity Report |  |  |  |
|  | Adv/2024/Jul/019 Phishing Attack |  |  |  |
|  | Adv/2024/Jul/020 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | Adv/2024/Jul/021 CobaltStrike Malware |  |  |  |
|  | Adv/2024/Jul/022 Weekly Mirai Activity Report |  |  |  |
|  | Adv/2024/Jul/024 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | Adv/2024/Jul/025 Malicious IPs |  |  |  |
|  | Adv/2024/Jul/026 Atomic Stealer |  |  |  |
|  | Adv/2024/Jul/027 Phishing Attack |  |  |  |
|  | Adv/2024/Jul/029 QuasarRAT Malware |  |  |  |
|  | Adv/2024/Jul/030 Racoon Malware |  |  |  |
|  | Adv/2024/Jul/031 RedLine Malware |  |  |  |
|  | Adv/2024/Jul/033 SocGholish Malware |  |  |  |
|  | Adv/2024/Jul/034 Ursnif Malware |  |  |  |
|  | Adv/2024/Jul/035 Qbot Malware |  |  |  |
|  | Adv/2024/Jul/036 Amadey Malware |  |  |  |
|  | Adv/2024/Jul/037 Redfoxtrot & SugarGh0st RAT |  |  |  |