# Standard Operating Procedure (SOP) Status for Threat Intelligence

## SOP Status of Operational Intelligence in February 2025

|  |  |  |  |
| --- | --- | --- | --- |
| Content of SOP | Detail | Stage | Responsible Person |
| Cyber Threat Operations (CTO) | 1st Modification of Latest Endorsement (Released on 26 Mar 2025)  Modified  •Phishing Email Handling   * As requested by AD(IT)(ITS)3, the categories "Unwanted" and "Neutral" have been removed. The new categories are "Spam" or "Phishing". * Justification: To unify the outcome of analyzing the reported email and prevent subjective conclusions. | Latest endorsement on 25 Feb 20251 | PwC, HKMA |
| Security Operations Centre (SOC) | Last Modification of Latest Version (in 05 Nov 2024) | Latest endorsement on 25 Feb 20251 | PwC, HKMA |
| Threat Hunting | 1st Modification of Latest Version (Released on 26 Mar 2025)  Modified  •Scope of Threat Hunting   * Expand the scope of threat hunting - Trending Threats (Not limited but include the following):   + Remote Access Tools   + InfoStealers * Provide a mapping of Remote Access Tools with corresponding threat actor groups for reference | Latest endorsement on 25 Feb 20251 | PwC, HKMA |
| Incident Response (IR) | Last Modification of Latest Version (in 31 Jul 2024) | Latest endorsement on 25 Feb 20251 | PwC, HKMA |

Remarks:

1 Since no further comment listed in February 2025 SOC Monthly Meeting on 25 Feb 2025, the latest version of SOP for Threat Intelligence – “HKMA Threat Intelligence SOP – 20250224” is endorsed.

# Cyber Threat Operations (CTO)

## 12.1 Monthly CVEs Summary

In February 2025, there were **2** high-security-level Common Vulnerabilities and Exposures (CVE), **7** medium-security-level CVE, **0** low-security-level CVE.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Severity Level | Source | Created | Jira Ticket No. | CVE number | Product | Summary | User Confirm Affected |
| High | PwC, CISA | 14/02/2025 | ITSSOC-9127 | CVE-2024-55591, CVE-2025-24472 | FortiOS  FortiProxy | Authentication Bypass Zero-Day Vulnerability in FortiOS and FortiProxy | **Yes** |
| High | PwC | 19/02/2025 | ITSSOC-9180 | CVE-2025-1094 | PostgreSQL | Actively Exploited PostgreSQL Quoting Problem with Encoding Errors Allows SQL Injection | **Yes** |
| Medium | PwC | 05/02/2025 | ITSSOC-9041 | CVE-2025-23114 | Veeam Backup Servers | Veeam Vulnerability Exposes Backup Servers to Remote Code Execution | N/A |
| Medium | PwC, GovCERT | 12/02/2025 | ITSSOC-9094 | CVE-2025-21391, CVE-2025-21418 | Microsoft Products | Multiple Vulnerabilities in Microsoft Products (February 2025) | N/A |
| Medium | PwC, GovCERT | 13/02/2025 | ITSSOC-9106 | CVE-2024-10644, CVE-2024-38657, CVE-2025-22467 | Ivanti Connect Secure (ICS) | Multiple Vulnerabilities in Ivanti Products | N/A |
| Medium | PwC | 13/02/2025 | ITSSOC-9111 | CVE-2025-0108 | PAN-OS | PAN-OS Authentication Bypass in the Management Web Interface Vulnerability | N/A |
| Medium | PwC | 19/02/2025 | ITSSOC-9186 | CVE-2025-26465, CVE-2025-26466 | OpenSSH | OpenSSH Vulnerabilities Allows Machine-in-the Middle and Denial-of-Service Attacks | N/A |
| Medium | PwC | 24/02/2025 | ITSSOC-9244 | CVE-2025-0111 | PAN-OS | PAN-OS Authenticated File Read Vulnerability in the Management Web Interface, Chained With CVE-2025-0108 | N/A |
| Medium | PwC | 27/02/2025 | ITSSOC-9307 | CVE-2025-0475 | GitLab CE/EE | GitLab CE/EE flaw in the Kubernetes Proxy Endpoint Leads to Cross-Site Scripting | N/A |

## 12.2 Monthly High Severity Level CVEs Tracking

In February 2025, there were **2** High Severity Level CVEs affecting HKMA. The affected systems/servers and their scheduled patch dates were tracked by the respective system owners.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CVE number | Product | Response from System Owner | | | | Recommendations by PwC |
| Internet Facing | Affected System/ Server IP | Solution | Target Solution Apply Date |
| CVE-2024-55591, CVE-2025-24472 | FortiOS  FortiProxy | No (Admin Interface) | IP  172.20.22.21  172.20.22.22  172.20.141.21  172.20.141.22 | Workaround as specified by advisory | Workaround: 15/01/2025 (Applied)  Patch:  17/02/2025 (Applied) | The System Owner should apply the both patch and workaround.  Justifications  By allowing only specified IP addresses to access the administrative interface and blocking all others, the workaround reduces the attack surface. The patch prevents systems remain exposed to potential attacks that can lead to unauthorized access. |
| CVE-2025-1094 | PostgreSQL | No | Name  JSM, IRIS | Upgrade to version 14.17 | Patch on 21/03/2025 | The System Owner should apply the patch.  Justifications  An attacker can leverage CVE-2025-1094 to control the operating system shell commands executed by psql. The patch addresses the root cause of the vulnerability by ensuring proper neutralization of quoting syntax in the affected functions. |
| Yes | Name  Event Management System  IP  172.31.234.105 | The project is finished, the VM will be shut down soon | VM Shut Down before 12/03/2025 |
| No | Name  SaltStack, Aria Operation, SDDC Manager, VRSLCM, vCenter, AAP, DPSA  IP  172.31.110.180  172.31.91.87  172.31.151.51  172.31.110.253  172.31.161.62 | Placed the remediation into the “within 180 days” | Within 180 days after acknowledging the vulnerability |

## Remark: Only the product running the affected version are shown.

## 12.3 Ongoing CVEs Remediation (Until 15 Mar 2025)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Jira Ticket Number | CVE Number | Product Impacted | Severity | System Owner Name(s) | Date Raised by SOC | SOC Follow-up Attempts (1,2,3) | Date of Acknowledgement | Date of Last Follow-up | CVE Relevant to HKMA | Affected System/ Server IP | Target Remediation Completion Date | Actual Remediation Date | Time from Date Raised to Date Acknowledged (days) | Time from Date Acknowledged to Date Remediated (days) | Aging of Actual Remediation Date to Target Remediation Completion Date (days) | Source of Alert |
| ITSSOC-8114 | CVE-2024-0012, CVE-2024-9474 | PAN-OS | High | Sr D(IT)(IS) | 15 Nov 2024 | 1 | 15 Nov 2024 | 1st Follow-up: 05 Dec 20241 | Yes | 172.22.48.101  172.22.48.102  172.22.48.105  172.22.48.111  172.22.48.112  172.22.49.101  172.22.49.102  172.22.49.105  172.22.49.111  172.22.49.112 | Q1 2025 | N/A | 1 | 1213 | N/A | PwC, GovCERT, CISA |
| ITSSOC-9180 | CVE-2025-1094 | PostgreSQL | High | AD(IT)(DP)1 | 1st Attempt: 19 Feb 2025  2nd Attempt: 21 Feb 2025  3rd Attempt: 25 Feb 2025 | 3 | 26 Feb 2025 | 1st Follow-up: 3 Mar 2025 | Yes | JSM, IRIS | 21 Mar 2025 | N/A | 7 | 183 | N/A | PwC |
| ITSSOC-9180 | CVE-2025-1094 | PostgreSQL | High | AD(IT)(PSM)1 | 1st Attempt: 19 Feb 2025  2nd Attempt: 21 Feb 2025  3rd Attempt: 25 Feb 2025  4th Attempt: 03 Mar 2025 | >3 | 04 Mar 2025 | 1st Follow-up: 5 Mar 2025; 11 Mar 2025 | Yes | 172.31.110.180  172.31.91.87  172.31.151.51  172.31.110.253  172.31.161.62 | Not yet  provided | N/A | 14 | 123 | N/A | PwC |

As of February 2025, there were **3** ongoing CVEs remediation efforts.

Remarks:

1 First Follow-Up: SOC requested information from the system owner regarding the CVE.

2 Second Follow-Up: SOC inquired about the system owner's patch status.

3 The timeframe is calculated up to 15 Mar 2025; additional days will continue to be added until the patch is completed.

## 12.4 Completed CVEs Remediation (Until 15 Mar 2025)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Jira Ticket Number | CVE Number | Product Impacted | Severity | System Owner Name(s) | Date Raised by SOC | SOC Follow-up Attempts (1,2,3) | Date of Acknowledgement | Date of Last Follow-up | CVE Relevant to HKMA | Affected System/ Server IP | Target Remediation Completion Date | Actual Remediation Date | Time from Date Raised to Date Acknowledged (days) | Time from Date Acknowledged to Date Remediated (days) | Aging of Actual Remediation Date to Target Remediation Completion Date (days) | Source of Alert |
| ITSSOC-7888 | CVE-2024-47575 | FortiManager | High | A(SYS)(IT)(IS)10 | 1st Attempt: 24 Oct 2024  2nd Attempt: 15 Nov 2024 | 2 | 15 Nov 2024 | 1st Follow-up: 29 Nov 20241  2nd Follow-up: 3 Jan 20252 | Yes | 172.20.22.23  172.20.141.23 | Dec 2024 | 12 Dec 2024 | 23 | 50 | 0 | PwC, GovCERT |
| ITSSOC-8780 | CVE-2024-55591, CVE-2025-24472 | FortiOS  FortiProxy | High | A(SYS)(IT)(IS)10 | 15 Jan 2025 | 1 | 15 Jan 2025 | 1st Follow-up: 16 Jan 2025; 20 Jan 20251  2nd Follow-up: 14 Feb 20252 | Yes | 172.20.22.21  172.20.22.22  172.20.141.21  172.20.141.22 | Feb 2025 | KCC: 8 Feb 2025  IFC: 15 Feb 2025 | 1 | 31 | 0 | PwC, GovCERT, CISA |
| ITSSOC-7772 | CVE-2024-23113 | FortiOS  FortiPAM  FortiProxy  FortiWeb | High | A(SYS)(IT)(IS)10 | 15 Oct 2024 | 1 | 17 Oct 2024 | 1st Follow-up: 29 Nov 20241 | Yes | 172.20.22.21  172.20.22.22  172.20.141.21  172.20.141.22 | Feb 2025 | 17 Feb 2025 | 3 | 125 | 0 | PwC, GovCERT |
| ITSSOC-9180 | CVE-2025-1094 | PostgreSQL | High | AD(IT)(AS2)2 | 1st Attempt: 19 Feb 2025  2nd Attempt: 21 Feb 2025  3rd Attempt: 25 Feb 2025  4th Attempt: 03 Mar 2025 | >3 | 05 Mar 2025 | 1st Follow-up: 6 Mar 2025; 7 Mar 2025 | Yes | 172.31.234.105 | Before 12 Mar 2025 | 10 Mar 2025 | 15 | 5 | 0 | PwC |

As of February 2025, there were **4** completed CVEs remediation efforts.

Remarks:

1 First Follow-Up: SOC requested information from the system owner regarding the CVE.

2 Second Follow-Up: SOC inquired about the system owner's patch status.

## 12.5 Major Threat Intelligence Report Highlight

This section shared major threat intelligence highlights for the past month.

1. LockBit Ransomware Deployed via Exposed & Exploited Windows Confluence Server
2. New Phishing Campaign Delivering Remote Desktop Protocol (RDP) files

12.6 Executive Summary

|  |  |
| --- | --- |
| Threat Intelligence | SOC Recommendation/Actionable Item |
| 1. LockBit Ransomware Deployed via Exposed & Exploited Windows Confluence Server | * TI on-site analyst conducts a threat hunt campaign against the LockBit Ransomware * No positive findings were observed in HKMA security solutions * All IoCs have been blocked |
| 1. New Phishing Campaign Delivering Remote Desktop Protocol (RDP) files | * TI on-site analyst conducts a threat hunt campaign against the LockBit Ransomware * No positive findings were observed in HKMA security solutions * All IoCs have been blocked |

1. LockBit Ransomware Deployed via Exposed & Exploited Windows Confluence Server

In early February 2024, a security breach was detected following the exploitation of a critical Confluence remote code execution vulnerability (CVE-2023-22527) on an exposed Windows server.

**Impact and Analysis**

This exploitation allowed the attacker to gain unauthorized access, enabling them to install AnyDesk for persistent access and create a local administrative account, which facilitated further exploitation. They utilized Mimikatz to harvest credentials, disabled security measures, and cleared event logs to conceal their activities. Through reconnaissance and lateral movement, they positioned themselves to execute further attacks within the network.

The breach escalated quickly, with sensitive data exfiltrated using Rclone to transfer files to MEGA.io cloud storage approximately 71 minutes after initial access. Within two hours of the intrusion, the attacker deployed LockBitransomware, employing both manual execution on critical servers and automated distribution methods like PDQ Deploy. This rapid deployment led to widespread file encryption and the creation of ransom notes, highlighting the efficiency and coordination of the attack strategy. Despite LockBit’s slowdown in frequency of attacks, their latest LockBit 4.0 strain indicates their intention to regain their cadence of attacks.

**Recommendations**

TI on-site analyst conducts a threat hunt campaign against the LockBit Ransomware. No positive findings were observed in HKMA security solutions, and all IoCs have been blocked.

Source: PwC Cyber Threat Intelligence Weekly Report [22 February 2025 – 28 February 2025]

1. New Phishing Campaign Delivering Remote Desktop Protocol (RDP) files

In late 2024, researchers tracked activity by the threat actor Midnight Blizzard and discovered their phishing campaign involving the use of Remote Desktop Files.

**Impact and Analysis**

By further monitoring online antivirus scanners for similar files, a new campaign that begun in late January 2025 was revealed. The campaign is noted to target organisations in government and education sectors, and still active as of mid-February 2025. The aforementioned campaign has not been linked to any threat actor and as such has been tracked by PwC Global Threat Intelligence as White Dev 199.

White Dev 199 has been seen to impersonate Ukretelecom, a Ukrainan telephone company and Rheinmetall a German automotive and arms manufacturer, though based on analysis of the network traffic researchers deduce the campaign is likely targeting clients of Rheinmetall rather than the company itself. We continue to observe a rise in reports of threat actors leveraging RDP files in their phishing campaigns.

**Recommendations**

TI on-site analyst conducts a threat hunt campaign against the Remote Desktop Protocol (RDP) files. No positive findings were observed in HKMA security solutions, and all IoCs have been blocked.

Source: PwC Cyber Threat Intelligence Weekly Report [15 February 2025 – 21 February 2025]

# Threat Hunting

## 13.1 Threat Hunting Relevance and Overview

In February 2025, a total of **14** threat hunting cases were handled. These included **8** government-targeted cases, **11** APAC-targeted cases, and **2** technology-related cases.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Created | Jira Ticket No. | Summary | Government Targeted | APAC Targeted | Technology Related |
| 03/02/2025 | ITSSOC-8991 | Threat Actors Exploit .Gov Websites for Phishing Campaigns | ✓ |  |  |
| 04/02/2025 | ITSSOC-9022 | Chinese-Linked APT Leverage Espionage Operation Against High-Value Targets in APAC Region | ✓ | ✓ |  |
| 06/02/2025 | ITSSOC-9045 | Actively Exploited Zero-Day Zip Vulnerability Bypassing Mark-of-the-Web Protection |  |  | ✓ |
| 12/02/2025 | ITSSOC-9091 | KillSec Ransomware Recent Threat Activities |  | ✓ |  |
| 13/02/2025 | ITSSOC-9119 | OceanLotus APT Group Uses New Memory Technique in Attacks Against China | ✓ | ✓ |  |
| 13/02/2025 | ITSSOC-9120 | OceanLotus APT Group Targeting High Value Organizations in China | ✓ | ✓ |  |
| 18/02/2025 | ITSSOC-9158 | Threat Actor Using Masqueraded Domains to Target Banking Clients (As Of 18 Feb) |  | ✓ |  |
| 19/02/2025 | ITSSOC-9187 | PDF-themed Campaign Using Compromised Infrastructure | ✓ | ✓ |  |
| 20/02/2025 | ITSSOC-9210 | FINALDRAFT Malware Exploits Outlook Drafts for Communication |  |  | ✓ |
| 24/02/2025 | ITSSOC-9242 | LummaC2 Malware Distributed Disguised as Total Commander Crack | ✓ | ✓ |  |
| 25/02/2025 | ITSSOC-9264 | New macOS Malware FrigidStealer Delivered via Web Inject Campaigns |  | ✓ |  |
| 25/02/2025 | ITSSOC-9265 | NOVA Stealer Distributed as a Disguised Contract Archive |  | ✓ |  |
| 26/02/2025 | ITSSOC-9284 | Lumma Stealer Malware Uncovers Unique Patterns in the Infostealer's Domain Clusters | ✓ | ✓ |  |
| 27/02/2025 | ITSSOC-9310 | New Evasive Linux Malware "Auto-Color" Targeting Governments | ✓ | ✓ |  |

## 13.2 Indicators of Compromise (IOCs) Blocked

In February 2025, a total of **14** threat hunting cases were handled.

In addition, this effort resulted in the blocking of **32** hashes, **110** domains or URLs, and **29** IP addresses. All Indicators of Compromise (IoCs) were blocked, with **no** left unblocked.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Created | Jira Ticket No. | Summary | Hits | Hash Blocked Count | Domain/URL Blocked Count | IP Blocked Count |
| 03/02/2025 | ITSSOC-8991 | Threat Actors Exploit .Gov Websites for Phishing Campaigns | No | 0 | 6 | 0 |
| 04/02/2025 | ITSSOC-9022 | Chinese-Linked APT Leverage Espionage Operation Against High-Value Targets in APAC Region | No | 3 | 4 | 9 |
| 06/02/2025 | ITSSOC-9045 | Actively Exploited Zero-Day Zip Vulnerability Bypassing Mark-of-the-Web Protection | No | 14 | 19 | 1 |
| 12/02/2025 | ITSSOC-9091 | KillSec Ransomware Recent Threat Activities | No | 1 | 0 | 3 |
| 13/02/2025 | ITSSOC-9119 | OceanLotus APT Group Uses New Memory Technique in Attacks Against China | No | 1 | 0 | 0 |
| 13/02/2025 | ITSSOC-9120 | OceanLotus APT Group Targeting High Value Organizations in China | No | 1 | 0 | 8 |
| 18/02/2025 | ITSSOC-9158 | Threat Actor Using Masqueraded Domains to Target Banking Clients (As Of 18 Feb) | No | 0 | 34 | 0 |
| 19/02/2025 | ITSSOC-9187 | PDF-themed Campaign Using Compromised Infrastructure | No | 3 | 20 | 2 |
| 20/02/2025 | ITSSOC-9210 | FINALDRAFT Malware Exploits Outlook Drafts for Communication | No | 3 | 4 | 0 |
| 24/02/2025 | ITSSOC-9242 | LummaC2 Malware Distributed Disguised as Total Commander Crack | No | 0 | 5 | 0 |
| 25/02/2025 | ITSSOC-9264 | New macOS Malware FrigidStealer Delivered via Web Inject Campaigns | No | 5 | 5 | 0 |
| 25/02/2025 | ITSSOC-9265 | NOVA Stealer Distributed as a Disguised Contract Archive | No | 1 | 0 | 0 |
| 26/02/2025 | ITSSOC-9284 | Lumma Stealer Malware Uncovers Unique Patterns in the Infostealer's Domain Clusters | No | 0 | 13 | 1 |
| 27/02/2025 | ITSSOC-9310 | New Evasive Linux Malware "Auto-Color" Targeting Governments | No | 0 | 0 | 5 |
| Total | | | | 32 | 110 | 29 |

# Phishing Email Alert Handling

## 14.1 Communications Division

There were 29 of reported emails from Communications Division in February 2025.

|  |  |  |
| --- | --- | --- |
| Created | Jira Ticket No. | Category |
| 04/02/2025 | ITSPEIR-3642 | Unwanted |
| 05/02/2025 | ITSPEIR-3644 | Phishing |
| 05/02/2025 | ITSPEIR-3646 | Spam |
| 05/02/2025 | ITSPEIR-3648 | Spam |
| 06/02/2025 | ITSPEIR-3650 | Neutral |
| 14/02/2025 | ITSPEIR-3657 | Phishing |
| 18/02/2025 | ITSPEIR-3659 | Neutral |
| 21/02/2025 | ITSPEIR-3661 | Spam |
| 21/02/2025 | ITSPEIR-3663 | Spam |
| 21/02/2025 | ITSPEIR-3665 | Spam |
| 21/02/2025 | ITSPEIR-3667 | Unwanted |
| 21/02/2025 | ITSPEIR-3669 | Spam |
| 21/02/2025 | ITSPEIR-3671 | Spam |
| 21/02/2025 | ITSPEIR-3673 | Spam |
| 21/02/2025 | ITSPEIR-3675 | Spam |
| 26/02/2025 | ITSPEIR-3680 | Phishing |
| 26/02/2025 | ITSPEIR-3682 | Spam |
| 26/02/2025 | ITSPEIR-3684 | Spam |
| 26/02/2025 | ITSPEIR-3686 | Unwanted |
| 26/02/2025 | ITSPEIR-3688 | Unwanted |
| 26/02/2025 | ITSPEIR-3690 | Spam |
| 26/02/2025 | ITSPEIR-3692 | Spam |
| 26/02/2025 | ITSPEIR-3694 | Phishing |
| 26/02/2025 | ITSPEIR-3696 | Phishing |
| 26/02/2025 | ITSPEIR-3698 | Phishing |
| 26/02/2025 | ITSPEIR-3700 | Spam |
| 27/02/2025 | ITSPEIR-3702 | Phishing |
| 27/02/2025 | ITSPEIR-3704 | Spam |
| 27/02/2025 | ITSPEIR-3705 | Spam |

## 14.2 Settlement Division

There were 3 of reported emails from Settlement Division in February 2025.

|  |  |  |  |
| --- | --- | --- | --- |
| Created | Jira Ticket No. | Summary | Category |
| 03/02/2025 | ITSPEIR-3640 | Spam Attachment | Spam |
| 10/02/2025 | ITSPEIR-3652 | Advertising Spam | Spam |
| 10/02/2025 | ITSPEIR-3654 | Financial Scam | Spam |

## 14.3 Overview

In February 2025, TI has acknowledged **32** suspicious email reports by users, confirming that there are **2** neutral emails, **4** unwanted emails, **19** spam emails, and **7** phishing emails. TI has sent out emails to the users who reported these emails, advising them to delete these emails and avoid clicking on any links or attachments within them. Additionally, instructions were provided on how to block future emails from the same sender to prevent further phishing attempts.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Neutral | Unwanted | Spam | Phishing |
| Communications Division | 2 | 4 | 16 | 7 |
| Settlements Division | 0 | 0 | 3 | 0 |
| Total | 2 | 4 | 19 | 7 |