Advisories

SR-030.062025: MyCERT Report - Cyber Incident Quarterly Summary Report - Q1 2025

10 Jun 2025 Report

Quarter 1 2025 Cyber Incident Summary Report

Cyber999 Incident Response Centre of CyberSecurity Malaysia

TLP WHITE

1.0 Introduction

The Cyber Incident Quarterly Summary Report Q1 2025 provides an overview of computer security incidents handled by the Cyber999 Incident Response Centre of CyberSecurity Malaysia in Q1 2025.

This quarterly Cyber Incident Report also highlights statistics of incidents dealt with by Cyber999 Incident Response Centre in Q1 2025 according to their categories and security alerts and advisories released in this quarter. It should be noted that the statistics provided in this report reflect only the total number of incidents reported and handled by the Cyber999 Incident Response Centre, excluding elements such as monetary value or aftermaths of the incidents. Computer security incidents dealt with by the Cyber999 Incident Response Centre involved IP addresses and domains from Malaysia.

CyberSecurity Malaysia works closely with ISPs, CERTs, Special Interest Groups (SIGs) and Law Enforcement Agencies (LEAs), from local and international, to remediate and mitigate computer security incidents affecting Malaysia's organisations and the public.

2.0 Trends Q1 2025

There were 33.59 million internet users in Malaysia at the start of 2024, while Malaysia was home to 28.68 million social media users in January 2024, equating to 83.1 percent of the total population [1]. Meanwhile, a total of RM3.18 billion has been lost to online scams involving more than 95,800 victims between 2021 and April 2024 [2]. In general, the Cyber999 Incident Response Centre receives incident reports from Internet users, members of the public, home users, small and medium enterprises (SMEs), industries, academia, and non-profit organisations (NGOs). We proactively seek and gather insights on cyber threats through partnerships and collaborations worldwide that could impact Internet users and organisations in Malaysia and aid in mitigating these threats. The Cyber999 Incident Response Centre received 1657 incidents in Q1 2025, compared to 1550 incidents in Q4 2024. This indicates a 7 percent increase in Q1 2025.

Tables 1 to 3 below provide details of the incidents, and their figures reported in Q4 2024 and Q1 2025.

Table 1: Comparison of Incidents Reported in Q4 2024 and Q1 2025

Categories of Incidents	Quarters		Percentage (%)
	Q4 2024	Q1 2025	
Denial of Service	3	6	100
Intrusion	75	132	76
Data Breach	151	195	29
Intrusion Attempt	97	101	3
Vulnerabilities Report	34	38	12

Malicious Codes	**42**	**43**	**2**
Fraud	**1108**	**1126**	**2**
Spam	**40**	**16**	**-60**
TOTAL	**1550**	**1657**	**7**

Table 2: Breakdown of Incidents Based on Months in Q1 2025

Categories of Incidents	**Jan**	**Feb**	**Mac**
Denial of Service	1	2	3
Intrusion	18	75	39
Data Breach	73	71	51
Intrusion Attempt	32	31	38
Vulnerabilities Report	14	8	16
Malicious Codes	9	11	23
Fraud	334	338	454
Spam	12	7	21
TOTAL	**493**	**543**	**645**

Table 3: Breakdown of categories and sub-categories of incidents in Q1 2025

Categories and Sub-categories of Incidents	**Jan**	**Feb**	**Mac**
Denial of Service			
Denial of Service – DoS	1	2	3
Fraud			
Fraud -- Bogus Email	8	10	10
Fraud – Business Email Compromise	1	2	3
Fraud – Fraud Site	2	2	4
Fraud – Impersonation & Spoofing	92	120	130
Fraud – Job Scam	4	3	13
Fraud – Love/Parcel Scam	0	0	3
Fraud -- Phishing	227	201	291
Vulnerabilities Report			
Vulnerabilities Report – Misconfiguration Information Disclosure	6	4	12

Vulnerabilities Report -- System	2	1	2
Vulnerabilities Report -- Web	6	3	2
Intrusion			
Intrusion – Account Compromise	14	19	31
Intrusion -- Defacement	4	56	8
Intrusion Attempt			
Intrusion Attempt – Login Brute Force	15	11	14
Intrusion Attempt – Port Scanning	0	0	0
Intrusion Attempt – Vulnerability Probes	17	20	24
Malicious Codes			
Malicious Codes – Botnet C&C	1	0	0
Malicious Codes – Malware	8	10	22
Malicious Codes – Malware Hosting	0	1	1
Content Related			
Content Related – Data Breach	73	71	51
Spam	7	5	4
TOTAL	**493**	**543**	**645**

Figure 1 illustrates and provides an overview of the incidents reported in Q1 2025 in a chart. Figure 2 illustrates the percentage of incidents based on their classification.

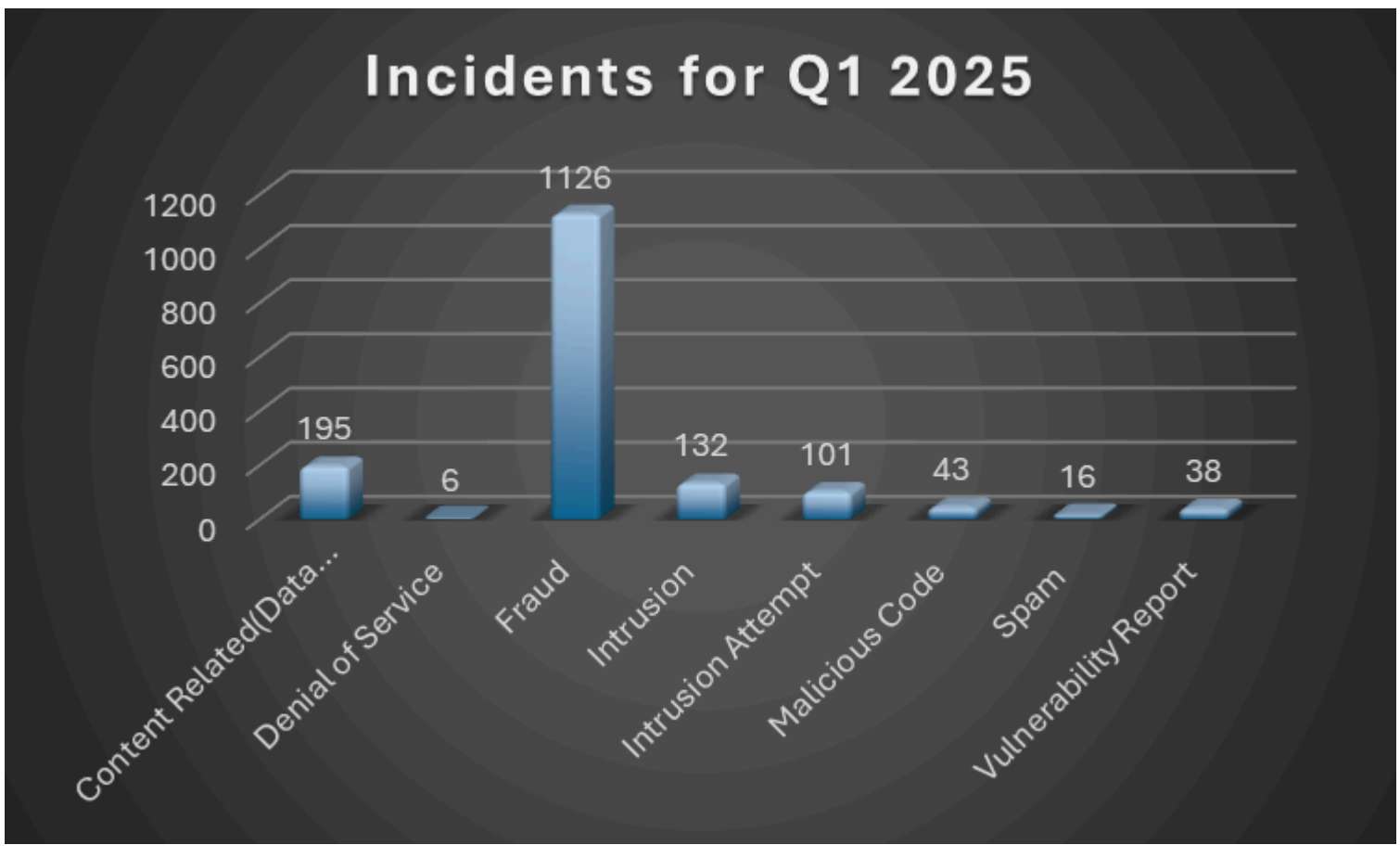

Figure 1: Breakdown of incidents based on categories in Q1 2025

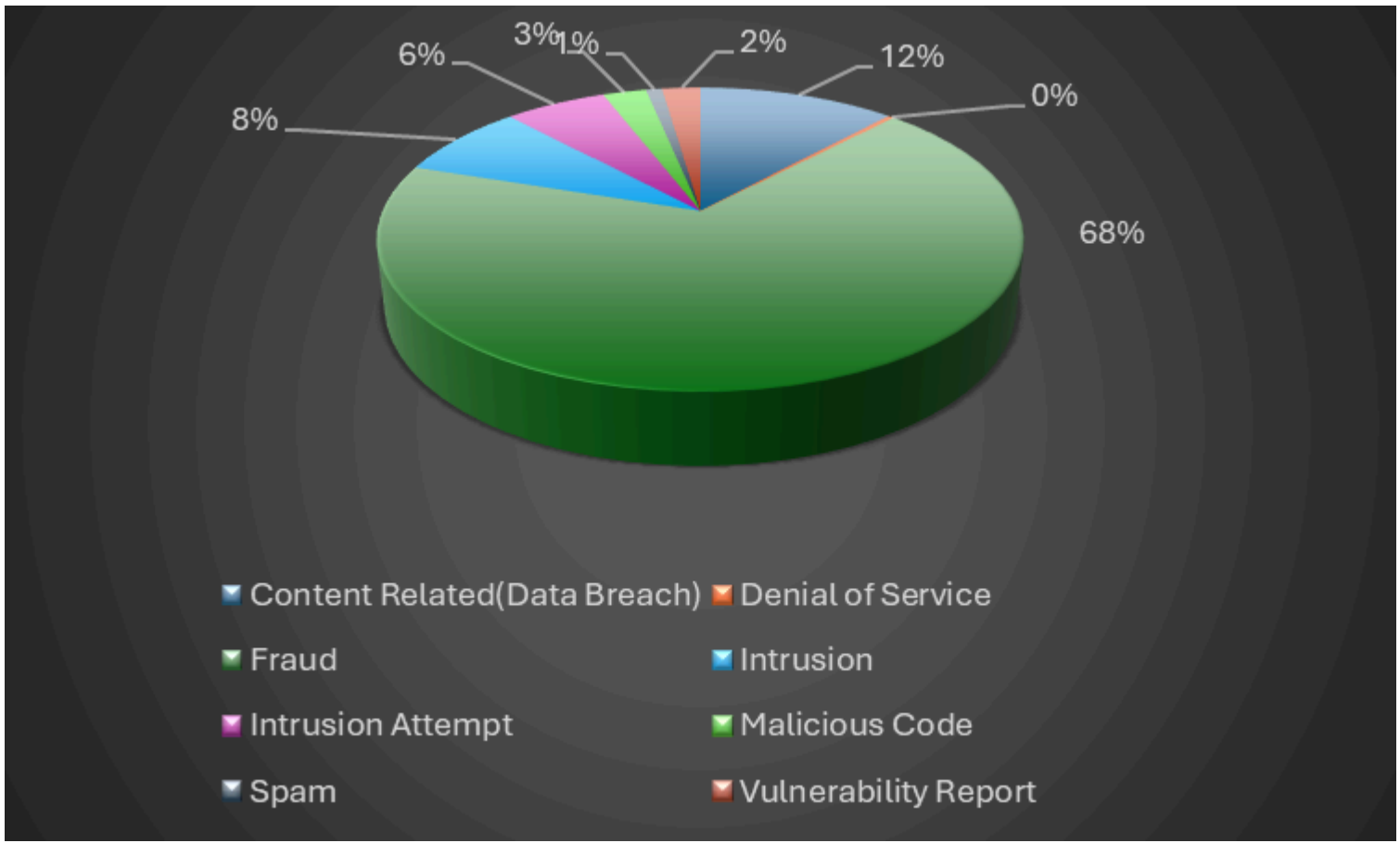

Figure 2: Percentage of incidents reported by categories in Q1 2025

Based on the above statistics, it is remarkable that most categories of incidents reported to us increased in Q1 2025 compared to Q4 2024. Intrusion incidents rose by 76 percent compared to Q4 2024. In Q1 2025, the most frequently reported incidents were Fraud, Intrusion, and Data Breach. Fraud accounted for the majority, representing 68 percent of all reported cases, followed by Intrusion at 12 percent and Data Breach at 8 percent.

Based on the current trends, fraud incidents will most likely continue to grow in Malaysia in 2025. Data breach incidents have slightly increased for this quarter. However, organisations and Internet users are urged to take proper security measures to prevent data breaches.

Meanwhile, for fraud incidents other than phishing URLs, new tactics and techniques in online scams that concatenate social engineering, and malicious code could grow in Malaysian cyberspace.

2.1 Top Fraud Incidents Reported in Q1 2025

Fraud continuously prevails within the community, targeting various citizens, end users and organisations, from students to professionals, large to small organisations. It has become a preferred method of criminals as awareness is still lacking among the public, making them an easier target. One thousand one hundred – twenty-six fraud incidents were handled this quarter, representing 2 percent increase compared to Q4 2024. All the fraud incidents were received from organisations and public users. The top fraud incidents reported to the Cyber999 Incident Response Centre are as follows:

Table 4: Top Fraud Incidents Reported in Q1 2025

Top Fraud incidents	Number of Incidents
Phishing	719
Impersonation and Spoofing	342
Bogus Email	28
Fraudulent Website	8
Job Scam	20
Business Email compromised – BEC scam	6
Love and parcel scam	3

Our statistics show that over three-quarters of fraud incidents reported are phishing, representing 68 percent of total fraud incidents reported in Q1 2025. We observed the following phishing trends in Malaysia based on the incidents reported to us. These trends are similar in the previous quarter, Q4 2024.

a.Contextualised and Localised Phishing Themes

Government Aid Scams: Phishing emails or SMS impersonate legitimate government programs (e.g., bantuan/sumbangan kerajaan), offering financial aid but requiring victims to provide personal details or click malicious links.

Fake Promotions and Discounts: Popular brands like Lazada, Shopee, or local retailers are spoofed, luring victims with fraudulent discounts or free vouchers.

Traffic Summons Scams: Messages claim unpaid police summons, providing fake payment links to steal financial credentials.

Subscription Services: Services like Netflix or Spotify are impersonated, tricking victims into renewing subscriptions or fixing payment issues on fake websites.

b.Mobile-Focused Phishing (Smishing and App-Based)

Smishing (SMS Phishing): Attackers send fraudulent SMS messages mimicking banks, e-wallets, or delivery services (e.g., J&T, Pos Malaysia) with malicious links.

c.Phishing Calls (Vishing)

Phone Scams: Attackers impersonate government agencies (e.g., police or LHDN, MCMC), banks, companies, or even CyberSecurity Malaysia, pressuring victims to disclose sensitive information. Common tactics include threats of legal action, account suspension, or overdue payments.

Therefore, Internet users and organisations must be vigilant when conducting online transactions or performing e-commerce transactions to avoid becoming victims of online fraud.

2.2 Top Malware Incidents Reported in Q1 2025

The top malware incidents include malware hosting, ransomware, malicious APK, backdoors, and trojans. The top reported malware incidents are related to malicious APKs. This type of incident is typically received from Internet banking users and sometimes from local financial institutions.

A **malicious APK** is an **Android Package (APK)** file containing **malware** designed to harm devices, steal data, or perform unauthorised actions. APK files are used to distribute and install applications on Android devices, and malicious versions exploit this format to spread malware. They often mimic popular apps (e.g., social media, games, or utilities) to trick users into downloading. Attackers may distribute these files through phishing emails, social media, fake websites, or third-party app stores.

Table 5: Types of Malicious APKs Reported in Q1 2025

Types of Malicious APK	Total
???pdf.app.apk	1
helpling COD	2
Encik Beku COD	1
cleaning service	3

The second top-reported incident within the malware category is malware hosting. Malware hosting primarily targeted vulnerable servers with outdated security patches and updates. These incidents are usually received from foreign entities, such as anti-virus vendors and special interest groups, regarding servers in Malaysia that are hosting malware. System Administrators must be vigilant and keep systems up to date with the latest patches and security updates to prevent servers from being compromised and hosting malware.

Ransomware incidents decreased in Q1 2025 compared to the previous quarter. We received 16 incidents in Q4 2024 and 12 in Q1 2025, indicating a **25% decrease**. Nevertheless, organisations must be vigilant about the decrease in ransomware incidents in this quarter. Ransomware is malicious software (malware) that infects a computer and restricts access until the requested ransom is paid. It is also considered one of the costliest and most devastating attacks, as it is enormous to recover all the data and rectify infected machines.

Our finding identified that businesses are most impacted by ransomware incidents in Malaysia, consistent across the globe. Active Directory(AD) servers have become primary targets in Malaysia. Compromising AD servers can significantly amplify the impact of a ransomware attack. Using tools like PsExec, Group Policy Objects (GPOs), or Windows Management Instrumentation (WMI) to execute ransomware on all connected systems. Ryuk and Conti have been observed targeting AD servers for mass deployment and faster network-wide encryption. We also observed attackers exploit vulnerabilities in virtualisation platforms like VMware, and ESXi servers can be targeted directly, allowing attackers to gain control over multiple VMs simultaneously. Ransomware operators use phishing attacks, brute force, or stolen credentials to access VM management consoles or servers. LockBit has been observed deploying scripts to attack VMware environments, including deleting backups and snapshots.

Looking at the current trends, ransomware incidents will continue to grow in Malaysia in 2025. The results show that reported ransomware incidents have slightly decreased in this quarter. Organisations and Internet users must always take proper security measures against ransomware incidents. Good backup management, password security, and cyber security awareness are essential in combating ransomware and other types of malware. Implementing the backup procedure, policy, and best practices among organisations and public users is also essential in mitigating ransomware attacks.

Table 6: Ransomware Variants Reported in Q1 2025

Types of Ransomware Variant	Number of Incidents
Akira	2
Annoy	1
Lockdown.syndicate	1
Loki Locker	1
HiddenTear	1
Medusa Locker	1
Bashe (APT73)	1
Funksec	1
NA	3

Apart from ransomware, we also handled incidents involving botnets that infected computers in Malaysia. A **botnet** (short for **robot network**) is a network of **computers or devices** infected by malicious programs and controlled by a single attacker called a **botmaster** or **bot herder**. These infected devices, called **bots** or **zombies**, enable the attacker to control them remotely. Botnets are commonly used in:

1. Distributed Denial-of-Service (DDoS) Attacks: to overwhelm a target system, server, or network, making it **unavailable to legitimate users**.
2. Massive Spam Campaigns: Sending large amounts of phishing or spam emails.
3. Credential Theft: Logging keystrokes to steal passwords or sensitive information.
4. Cryptojacking: Using infected devices to mine cryptocurrency without consent.

Below is the list of top botnets that infected computers, primarily belonging to individuals and organisations in Malaysia, as reported to the Cyber999 Incident Response Centre in Q1 2025:

Table 7: Types of Botnets Reported in Q1 2025

Types of Botnets	Total Infected IPs
android.vo1d	1,014,302
avalanche-andromeda	293,104
socks5systemz	59,174

ngioweb	46,195
vipersoftx	29,895
tsifiri	28,053
sality	18,608
adload	12,716
downadup	11,913
pykspa	9,763

Apart from ransomware, botnets and malware hosting, we also handled incidents related to infostealer in Q1 2025. Infostealer is malicious software created to breach computer systems and steal sensitive information, including login details. Generally, data from the infostealers contained login credentials from various sources, including information saved on web browsers (such as passwords and credit logins), auto-filled logins, FTP clients, email apps, instant messaging clients, and VPNs.

Below is a list of infostealers associated with data breach reported to us in Q1 2025:

Table 8: Info stealers reported in Q1 2025

Types of Info Stealers	Number of Incidents
Satanic Cloud Stealer	1
LummaC2	3
Starlink	7
Blum ULP	1

2.3 Data Breach Incidents Growing in Malaysia

Data breach incidents are growing in Malaysia, with a nearly 29 percent increase this quarter, underscoring the need for better security measures to ensure national security and public trust. High-profile breaches often involve massive datasets, including personal identifier information (PII) like identification numbers, addresses, and financial details, and often involve PII from national databases. Serious security measures must consistently be implemented to prevent and mitigate data breaches, especially for personal data.

We are also observing a trend where perpetrators exfiltrate or steal sensitive data from organisations and hold the data hostage, in some cases after ransomware attacks. Perpetrators will then threaten the organisation to release or sell the data on the dark web unless the organisation pays ransom within a timeframe set by the perpetrators. In the case of extortion by perpetrators, we always advise organisations to refer the matter to the LEAs, such as the police, for assistance. Other trends we observed in this quarter include resurfacing of previous data breaches. Perpetrators claimed and posted on the dark web that they have breached data belonging to specific organisations. However, our analysis confirmed these are resurfaces of previous data breaches that happened a few years back and not new breaches.

Table 9: Data Breaches Reported in Q1 2025

Types of Data Breach	Description
Personal Identifier Information (PII)	Full name, identity card numbers, home address, age, handphone number, date of birth, and salary.

Account Credential	Username and password of email accounts, username and password of Internet banking accounts.
Appliances Credential	Admin panel access, Joomla, wordpress, ftp access, wp-admin access and etc.

3.0 Security Advisories and Alerts Released in Q1 2025

In Q1 2025, the Cyber999 Incident Response Centre issued 73 Security Advisories and one Alerts, each with descriptions, mitigation steps, and recommendations for organisations and Internet users to follow. The security advisories involved Mozilla, Microsoft, Apple, VMware, and several other CVEs listed in Table 10. The security alerts concern growing online fraud and malware threats that we identified as potentially serious to citizens and organisations in Malaysia. If not correctly identified and mitigated, such threats could have serious consequences for citizens and organisations.

Table 10: List of Significant CVEs in Q1 2025

Here is the table with the CVEs and their descriptions:

CVE ID	Description
CVE-2015-2051	The D-Link DIR-645 Wired/Wireless Router Rev. Ax with firmware 1.04b12 and earlier allows remote attackers to execute arbitrary commands via a GetDeviceSettings action to the HNAP interface.
CVE-2019-10891	An issue was discovered in D-Link DIR-806 devices. There is a command injection in function hnap_main, which calls system() without checking the parameter that can be controlled by user and finally allows remote attackers to execute arbitrary shell commands with a special HTTP header.
CVE-2022-37056	D-Link GO-RT-AC750 GORTAC750_revA_v101b03 and GO-RT-AC750_revB_FWv200b02 is vulnerable to Command Injection via /cgibin, hnap_main,
CVE-2024-33112	Command injection vulnerability in D-Link DIR-845L router v1.01KRb03 and earlier via the hnap_main() function.
CVE-2024-56337	Time-of-check Time-of-use (TOCTOU) Race Condition in Apache Tomcat Due to incomplete mitigation of CVE-2024-50379, affecting versions 9.0.0.M1 through 9.0.97, 10.1.0-M1 through 10.1.33, and 11.0.0-M1 through 11.0.1.

CVE-2024-50379	TOCTOU Race Condition during JSP compilation in Apache Tomcat Permitting remote code execution on case-insensitive file systems when the default servlet is enabled for write. Affects versions 9.0.0.M1 through 9.0.97, 10.1.0-M1 through 10.1.33, and 11.0.0-M1 through 11.0.1.
CVE-2025-22217	Avi Load Balancer contains an unauthenticated blind SQL Injection vulnerability which was privately reported to VMware. Patches are available to remediate this vulnerability in affected VMware products. A malicious user with network access may be able to use specially crafted SQL queries to gain database access.
CVE-2025-0611	Object corruption in V8 in Google Chrome Allowing remote attackers to potentially exploit heap corruption via crafted HTML pages.
CVE-2025-0612	Out-of-bounds memory access in V8 in Google Chrome Allowing remote attackers to potentially exploit heap corruption via crafted HTML pages.
CVE-2025-0444	Use-after-free vulnerability in Skia in Google Chrome Allowing remote attackers to potentially exploit heap corruption via crafted HTML pages.
CVE-2025-0445	Use after free in V8 in Google Chrome Allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2025-0451	Inappropriate implementation in Extensions API in Google Chrome Allowing remote attackers to perform UI spoofing via crafted Chrome Extensions.
CVE-2024-11187	Potential for resource exhaustion in BIND 9 due to responses containing numerous records in the Additional section, affecting versions 9.11.0 through 9.11.37, 9.16.0 through 9.16.50, 9.18.0 through 9.18.32, 9.20.0 through 9.20.4, and 9.21.0 through 9.21.3.
CVE-2024-12705	Clients using DNS-over-HTTPS (DoH) can exhaust a DNS resolver's CPU and/or memory by flooding it with crafted valid or invalid HTTP/2 traffic, affecting BIND 9 versions 9.18.0 through 9.18.32, 9.20.0 through 9.20.4, and 9.21.0 through 9.21.3.

CVE-2025-24118	The issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.4, macOS Sequoia 15.3, macOS Sonoma 14.7.3. An app may be able to cause unexpected system termination or write kernel memory.
CVE-2025-0999	Heap buffer overflow in V8 Allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2025-1426	Heap buffer overflow in GPU Allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2025-1006	Use-after-free in Network Allowed a remote attacker to potentially exploit heap corruption via a crafted web app
CVE-2025-21415	Azure AI Face Service vulnerability Authentication bypass by spoofing in Azure AI Face Service allows an authorized attacker to elevate privileges over a network.
CVE-2025-21396	Microsoft Account platforms vulnerability Missing authorization in Microsoft Account allows an unauthorized attacker to elevate privileges over a network.
CVE-2025-23114	A vulnerability in Veeam Updater component allows Man-in-the-Middle attackers to execute arbitrary code on the affected server. This issue occurs due to a failure to properly validate TLS certificate.
CVE-2025-21391	Windows Storage Elevation of Privileges Vulnerability.
CVE-2025-21418	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability.
CVE-2025-21194	Microsoft Surface Security Feature Bypass Vulnerability.
CVE-2025-21377	NTLM Hash Disclosure Spoofing Vulnerability.
CVE-2025-21198	Microsoft High Performance Compute (HPC) Pack Remote Code Execution Vulnerability.
CVE-2025-21376	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
CVE-2025-21381	Microsoft Excel Remote Code Execution Vulnerability.

CVE-2025-0995	Use-after-free flaw in Chrome’s V8 JavaScript engine Allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page
CVE-2025-0996	Inappropriate implementation in the Browser UI. Allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page
CVE-2025-0997	Use-after-free vulnerability in the Navigation component. Allowed a remote attacker to potentially exploit heap corruption via a crafted Chrome Extension.
CVE-2025-0998	Out-of-bounds memory access in V8.
CVE-2025-21420	Windows Disk Cleanup Tool Elevation of Privilege Vulnerability
CVE-2025-20111	A vulnerability in the health monitoring diagnostics of Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches in standalone NX-OS mode could allow an unauthenticated, adjacent attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of specific Ethernet frames. An attacker could exploit this vulnerability by sending a sustained rate of crafted Ethernet frames to an affected device. A successful exploit could allow the attacker to cause the device to reload.
CVE-2024-43093	In shouldHideDocument of ExternalStorageProvider.java, there is a possible bypass of a file path filter designed to prevent access to sensitive directories due to incorrect unicode normalization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.
CVE-2024-50302	In the Linux kernel, the following vulnerability has been resolved: HID: core: zero-initialize the report buffer Since the report buffer is used by all kinds of drivers in various ways, let's zero-initialize it during allocation to make sure that it can't be ever used to leak kernel memory via specially crafted report.
CVE-2025-23209	Craft is a flexible, user-friendly CMS for creating custom digital experiences on the web and beyond. This is a remote code execution (RCE) vulnerability that affects Craft 4 and 5 installs where your security key has already been compromised. Anyone running an unpatched version of Craft with a compromised security key is affected. This vulnerability has been patched in Craft 5.5.8 and 4.13.8. Users who cannot update to a patched version, should rotate their security keys and ensure their privacy to help migitgate the issue.

CVE-2024-39328	Insecure Permissions in Atos Eviden IDRA and IDCA before 2.7.0. A highly trusted role (Config Admin) could exceed their configuration privileges in a multi-partition environment and access some confidential data. Data integrity and availability is not at risk.
CVE-2024-39327	Incorrect Access Control vulnerability in Atos Eviden IDRA before 2.6.1 could allow the possibility to obtain CA signing in an illegitimate way.
CVE-2024-12510	Lightweight Directory Access Protocol (LDAP) vulnerability. If LDAP settings are accessed, authentication could be redirected to another server, potentially exposing credentials. This requires admin access and an active LDAP setup.
CVE-2024-12511	SMB/FTP services vulnerability. With address book access, SMB/FTP settings could be modified, redirecting scans and possibly capturing credentials. This requires enabled scan functions and printer access.
CVE-2025-24989	Vulnerability in Microsoft Power Pages. Allows an unauthorized attacker to elevate privileges over a network potentially bypassing the user registration control. This vulnerability has already been mitigated in the service and all affected customers have been notified. This update addressed the registration control bypass. Affected customers have been given instructions on reviewing their sites for potential exploitation and clean up methods. If you've not been notified this vulnerability does not affect you.
CVE-2025-1920	Type Confusion in V8. Allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page
CVE-2025-2135	Type Confusion in V8. Allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page
CVE-2025-2136	Use-after-free in Inspector. Allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page

CVE-2025-2137	Out-of-bounds read in V8. Allowed a remote attacker to perform out of bounds memory access via a crafted HTML page
CVE-2025-24983	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability. Allows an authorized attacker to elevate privileges locally.
CVE-2025-24984	Windows NTFS Information Disclosure Vulnerability. Insertion of sensitive information into log file in Windows NTFS allows an unauthorized attacker to disclose information with a physical attack.
CVE-2025-24985	Windows Fast FAT File System Driver Remote Code Execution Vulnerability Allows an unauthorized attacker to execute code locally.
CVE-2025-24991	Windows NTFS Information Disclosure Vulnerability. Allows an authorized attacker to disclose information locally.
CVE-2025-24993	Windows NTFS Remote Code Execution Vulnerability. Allows an unauthorized attacker to execute code locally.
CVE-2025-26633	Microsoft Management Console Security Feature Bypass Vulnerability. Allows an unauthorized attacker to bypass a security feature locally.
CVE-2025-26630	Microsoft Access Remote Code Execution Vulnerability. Use after free in Microsoft Office Access allows an unauthorized attacker to execute code locally.
CVE-2025-2783	Incorrect handle provided in unspecified circumstances in Mojo in Google Chrome on Windows Allowed a remote attacker to perform a sandbox escape via a malicious file.

CVE-2025-24813	Path Equivalence: 'file. Name' (Internal Dot) leading to Remote Code Execution and/or Information disclosure and/or malicious content added to uploaded files via write enabled Default Servlet in Apache Tomcat. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.2, from 10.1.0-M1 through 10.1.34, from 9.0.0.M1 through 9.0.98. If all of the following were true, a malicious user was able to view security sensitive files and/or inject content into those files: - writes enabled for the default servlet (disabled by default) - support for partial PUT (enabled by default) - a target URL for security sensitive uploads that was a sub-directory of a target URL for public uploads - attacker knowledge of the names of security sensitive files being uploaded - the security sensitive files also being uploaded via partial PUT If all of the following were true, a malicious user was able to perform remote code execution: - writes enabled for the default servlet (disabled by default) - support for partial PUT (enabled by default) - application was using Tomcat's file based session persistence with the default storage location - application included a library that may be leveraged in a deserialization attack Users are recommended to upgrade to version 11.0.3, 10.1.35 or 9.0.99, which fixes the issue.

4.0 Conclusion

Overall, the number of computer security incidents reported to the Cyber999 Incident Response Centre in Q1 2025 was 1,657, representing an increase of about 7% compared to Q4 2024. No significant or severe incidents were observed during this quarter. Nevertheless, organisations and individuals must always be vigilant with readiness and preventive and mitigation steps against potential threats. Perpetrators are very motivated, eager, and determined to use new and sophisticated tactics and techniques to execute cyber-attacks.

Hence, we strongly recommend that all internet users be constantly aware of today's cybercrime trends and adhere to the best cyber hygiene practices. This also includes secure handling of emails from unknown sources, safe web browsing, purchasing goods online, and using social media applications. Users must keep systems up to date with the latest security patches and updates to prevent their computers from being compromised or infected with malware. Always check the legibility of the applications, portal, merchants, services, and products before conducting any online transaction.

As the complexity of cyber threats continues to increase, organisations and individuals could be potential targets if they are not equipped with security awareness. Providing security awareness campaigns to citizens and organisations is among the best efforts to improve national cyber security and public trust.

Malaysian Internet users and organisations may contact us to report cyber security incidents at the below contact:

E-mail: cyber999[at]cybersecurity.my
Phone: 1-300-88-2999 (monitored during business hours)
Mobile: +60 19 2665850 (24x7 call incident reporting)
Business Hours: Mon - Fri 08:30 -17:30 MYT
Web: https://www.cybersecurity.my

5.0 References:

[1] https://datareportal.com/reports/digital-2024-malaysia (https://datareportal.com/reports/digital-2024-malaysia)

[2] https://www.nst.com.my/business/economy/2024/08/1090337/rm32b-lost-online-scams-between-2021-and-april-2024-gobind (https://www.nst.com.my/business/economy/2024/08/1090337/rm32b-lost-online-scams-between-2021-and-april-2024-gobind)

-- Year --

-- Type --

Type here ...

SEARCH

Popular Advisories

MA-1028.022024: Scam Call Impersonation (/portal/advisory?id=MA-1028.022024)

MA-834.052022: SMSSpy campaign to steal Malaysian banking user credential (/portal/advisory?id=MA-834.052022)

MA-782.042020: Online Video Tele-conferencing (VTC) Application Security Guidelines (/portal/advisory?id=MA-782.042020)

MA-797.122020: MyCERT Alert – Misuse of Personal Data by Unlicensed Online Loan Provider (/portal/advisory?id=MA-797.122020)

MA-798.122020: Mass Web Defacement (/portal/advisory?id=MA-798.122020)

Archives

January, 2026 (/portal/advisories?id=431fab9c-d24c-4a27-ba93-e92edafdefa5&month=2026-01)

update (/portal/advisories?id=431fab9c-d24c-4a27-ba93-e92edafdefa5&keyword=update)security (/portal/advisories?id=431fab9c-d24c-4a27-ba93-e92edafdefa5&keyword=security)vulnerability (/portal/advisories?id=431fab9c-d24c-4a27-ba93-e92edafdefa5&keyword=vulnerability)Microsoft (/portal/advisories?id=431fab9c-d24c-4a27-ba93-e92edafdefa5&keyword=Microsoft)microsoft (/portal/advisories?id=431fab9c-d24c-4a27-ba93-e92edafdefa5&keyword=microsoft)mozilla (/portal/advisories?id=431fab9c-d24c-4a27-ba93-e92edafdefa5&keyword=mozilla)phishing (/portal/advisories?id=431fab9c-d24c-4a27-ba93-e92edafdefa5&keyword=phishing)malware (/portal/advisories?id=431fab9c-d24c-4a27-ba93-e92edafdefa5&keyword=malware)cisco (/portal/advisories?id=431fab9c-d24c-4a27-ba93-e92edafdefa5&keyword=cisco)firefox (/portal/advisories?id=431fab9c-d24c-4a27-ba93-e92edafdefa5&keyword=firefox)ransomware (/portal/advisories?id=431fab9c-d24c-4a27-ba93-e92edafdefa5&keyword=ransomware)thunderbird (/portal/advisories?id=431fab9c-d24c-4a27-ba93-e92edafdefa5&keyword=thunderbird)apple (/portal/advisories?id=431fab9c-d24c-4a27-ba93-e92edafdefa5&keyword=apple)vmware (/portal/advisories?id=431fab9c-d24c-4a27-ba93-e92edafdefa5&keyword=vmware)adobe (/portal/advisories?id=431fab9c-d24c-4a27-ba93-e92edafdefa5&keyword=adobe)iOS (/portal/advisories?id=431fab9c-d24c-4a27-ba93-e92edafdefa5&keyword=iOS)fortinet (/portal/advisories?id=431fab9c-d24c-4a27-ba93-e92edafdefa5&keyword=fortinet)iPadOS (/portal/advisories?id=431fab9c-d24c-4a27-ba93-e92edafdefa5&keyword=iPadOS)holiday (/portal/advisories?id=431fab9c-d24c-4a27-ba93-e92edafdefa5&keyword=holiday)macOS (/portal/advisories?id=431fab9c-d24c-4a27-ba93-e92edafdefa5&keyword=macOS)

MyCERT
Malaysia Computer Emergency Response Team

Malaysia Computer Emergency Response Team (MyCERT) was formed on January 13, 1997 and started its full operation on March 1, 1997. Operating from the office of CyberSecurity Malaysia, MyCERT provides a point of reference for the Internet community in Malaysia to deal with computer security incidents.

(https://www.facebook.com/mycert.org.my/)

Quick Links

» Who we are (/portal/full?id=d8032294-04b2-4ba0-9e46-62c898bb4983)
» Core functions (/portal/full?id=2fc63821-302f-4722-861e-9ba14d8abd59)
» Contact us (/portal/full?id=f210fe13-3a27-4b03-9f79-8822e40734f2)
» PGP key (/portal/full?id=04ef640c-52e3-46f8-9b2d-196d60a6e7ba)
» Blog (/portal/full?id=0624654c-b676-47ff-bd69-212ff3ba3823)
» Advisories (/portal/advisories?id=431fab9c-d24c-4a27-ba93-e92edafdefa5)
» Cyber999 help Centre (/portal/full?id=9eb77829-7dd4-4180-814f-de3a539b7a01)
» Cyber Threat Research Centre (/portal/full?id=e4df37f1-6392-4701-be42-78c6da82f52a)
» Incident Statistics (/portal/statistics?id=b75e037d-6ee3-4d11-8169-66677d694932)

Get in Touch

Malaysia Emergency Response Team (MyCERT)
CyberSecurity Malaysia, Level 7 Tower 1,
Menara Cyber Axis, Jalan Impact,
63000 Cyberjaya, Selangor Darul Ehsan, MALAYSIA
1-300-88-2999 (Office Hours)
+6019 - 2665850 (24x7)
cyber999 [at] cybersecurity.my (mailto:cyber999 [at] cybersecurity.my)
https://www.mycert.org.my