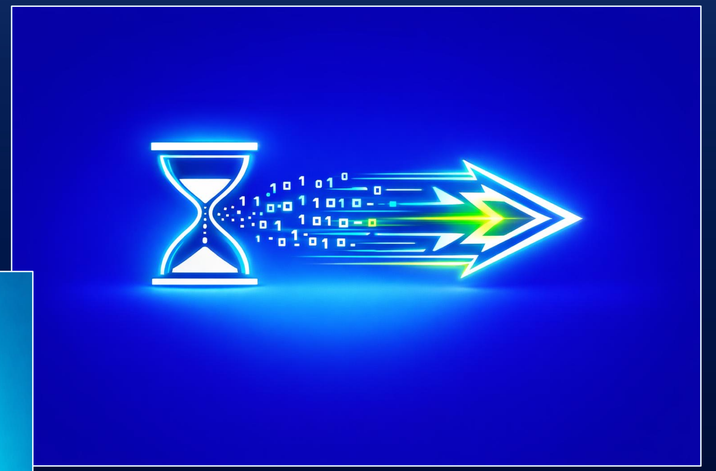
FACTS, NOT FADS
OT/IOT SECURITY INSIGHTS FROM ASEAN'S CYBER FRONTLINES

ALEXEY KLEYMENOV
THREAT INTELLIGENCE MANAGER
NOZOMI NETWORKS

THE WORLD IS CHANGING AT A FASTER PACE

AI is everywhere

Cyberattacks **on critical infrastructure** have become the new norm



Time-to-compromise is shrinking

HOW CAN WE GET READY?

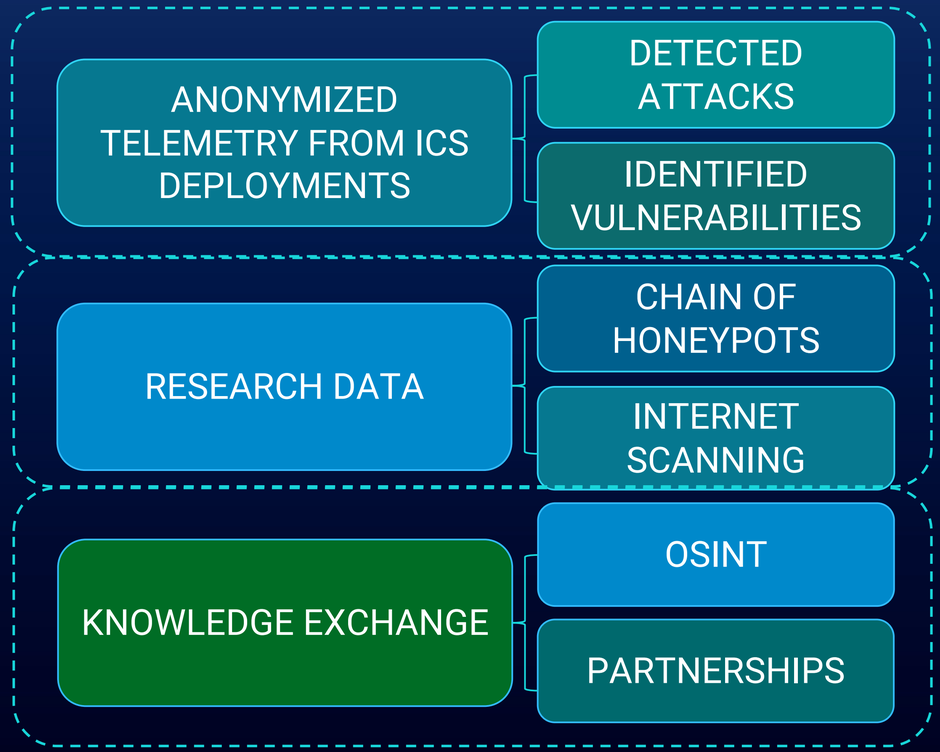
AGENDA

- One Year Later: **What's Different**?
- **Top Techniques** Used by Attackers: Global Trends vs ASEAN Realities
- **Top Malware** Observed in the Region
- Local **Vulnerability Landscape** and **Wireless Threats**
- **IoT Botnet** Activity in ASEAN Environments
- Latest actionable **recommendations**

ONE YEAR LATER: WHAT'S DIFFERENT?

- Continuous shift from **high volume cybercrime** to **targeted operations**
  - **Critical infrastructure** receives increasing interest from attackers
  - Operation **CYBER GUARDIAN** in Singapore to combat **UNC3886** APT actor
- **Geopolitical** events are now constantly intertwined with **cyberattacks**
  - Attackers targeting cameras and PLCs in the **Iranian conflict**
  - **Blurring lines** between state actors, cybercriminals and hacktivists
- AI-powered attacks are **the new normal**
  - More **reliable** and **versatile** tools can be created **faster**
  - **A lower barrier** to entry for **new** actors and existing actors exploring **new domains**

UNDERSTANDING THE DATA ORIGINS

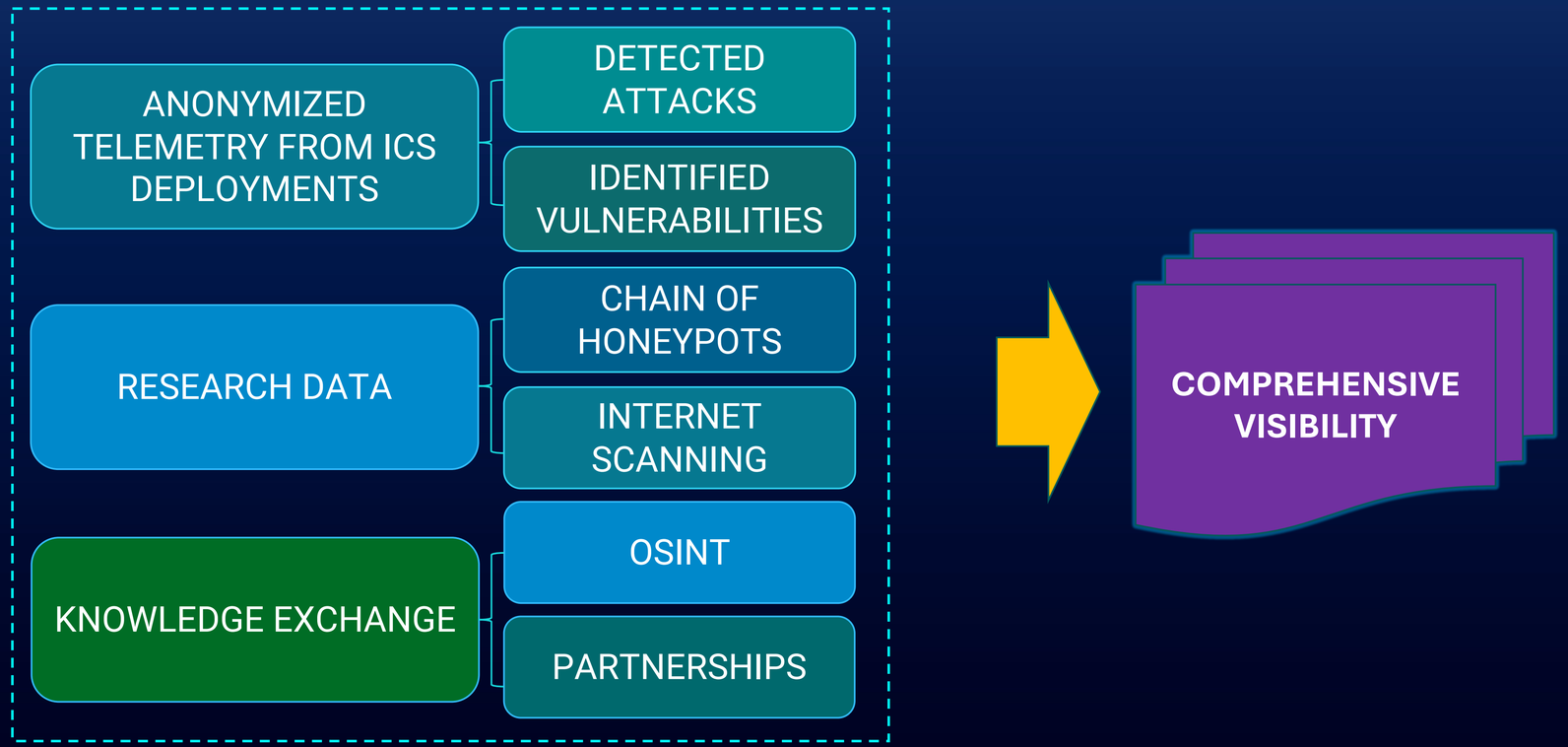


- Data from 20 sectors and multiple sub-sectors
- 15 sub-sectors are covered in the ASEAN region

- Sensors simulating vulnerable devices
- Completely independent of customers' environments

- Automated data consumption
- Covers both new data and ongoing changes

UNDERSTANDING THE DATA ORIGINS



TOP TECHNIQUES USED BY ATTACKERS: GLOBAL TRENDS VS ASEAN REALITIES

Technique ID	Technique Name	Tactics	Percentage
T0812	Default Credentials	Lateral Movement	16.7%
T0859	Valid Accounts	Persistence; Lateral Movement	16.7%
T0846	Remote System Discovery	Discovery	14.9%
T0841	Network Service Scanning	Discovery	14.9%
T1110	Brute Force	Credential Access	14.2%

Top 5 MITRE techniques in ASEAN in 1H 2026

Technique ID	Technique Name	Tactics	Percentage
T1498	Network Denial of Service	Impact	10.3%
T0814	Denial of Service	Inhibit Response Function	10.2%
T1110	Brute Force	Credential Access	10.8%
T0846	Remote System Discovery	Discovery	8.38%
T0841	Network Service Scanning	Discovery	8.38%

Top 5 MITRE techniques globally in 1H 2026

- Attackers are still **establishing a foothold** here (Discovery, Lateral Movement tactics)
- Clear interest in using **compromised valid accounts** and **default credentials** vs exploits
- Preference for **stealthy operations** delaying the Impact stage

TOP TECHNIQUES USED BY ATTACKERS: REGIONAL DRILLDOWN

Ranking based on the number of alerts raised per organization:

Top targeted countries in ASEAN in 1H 2026	*Top targeted countries in ASEAN in 1H 2025*
↑ •Philippines	•Malaysia
↑ •Vietnam	•Philippines
● •Singapore	•Singapore
● •Thailand	•Thailand
● •Indonesia	•Indonesia

TOP TECHNIQUES USED BY ATTACKERS: REGIONAL DRILLDOWN

ID	Name	Tactics	%
T0846	Remote System Discovery	Discovery	28.5%
T0841	Network Service Scanning	Discovery	28.5%
T0812	Default Credentials	Lateral Movement	14.6%
T0859	Valid Accounts	Persistence; Lateral Movement	14.6%
T1110	Brute Force	Credential Access	5.91%

ID	Name	Tactics	%
T1110	Brute Force	Credential Access	25.0%
T0812	Default Credentials	Lateral Movement	15.1%
T0859	Valid Accounts	Persistence; Lateral Movement	15.1%
T1498	Network DoS	Impact	12.2%
T0814	Denial of Service	Inhibit Response Function	12.2%

ID	Name	Tactics	%
T1200	Hardware Additions	Initial Access	91.7%
T0846	Remote System Discovery	Discovery	3.25%
T0841	Network Service Scanning	Discovery	3.25%
T1557	Adversary-in-the-Middle	Credential Access; Collection	0.48%
T0812	Default Credentials	Lateral Movement	0.35%

ID	Name	Tactics	%
T1110	Brute Force	Credential Access	25.8%
T1498	Network DoS	Impact	15.4%
T0814	Denial of Service	Inhibit Response Function	15.4%
T0812	Default Credentials	Lateral Movement	15.3%
T0859	Valid Accounts	Persistence; Lateral Movement	15.3%

TOP TECHNIQUES USED BY ATTACKERS: SECTOR INSIGHTS

Top industries in ASEAN where companies experienced the highest number of alerts per organization in 1H 2026:

- **Manufacturing**
- **Consumer Services**
- **Business Services**

In 1H 2025, **Transportation** was the most targeted sector in the region

Each industry features its own unique set of top TTPs used against it

ID	Name	Tactics	%
T0812	Default Credentials	Lateral Movement	17.0%
T0859	Valid Accounts	Persistence; Lateral Movement	17.0%
T0846	Remote System Discovery	Discovery	15.1%
T0841	Network Service Scanning	Discovery	15.1%
T1110	Brute Force	Credential Access	14.3%

ID	Name	Tactics	%
T1110	Brute Force	Credential Access	23.0%
T0846	Remote System Discovery	Discovery	14.5%
T0841	Network Service Scanning	Discovery	14.5%
T1071	Application Layer Protocol	Command And Control	11.9%
T1095	Non-Application Layer Protocol	Command And Control	11.9%

TOP MALWARE OBSERVED IN THE REGION

Malware family	Malware category	%
DoublePulsar	RAT	73.8%
ANDROMEDA	TROJAN	13.3%
Generic	TROJAN	10.0%
Conficker	WORM	0.95%
njRAT	RAT	0.67%

Threat actor	Associated country	%
Mustang Panda	China	38.9%
APT28	Russia	29.3%
APT39	Iran	8.92%
APT41	China	3.82%
MuddyWater	Iran	1.91%

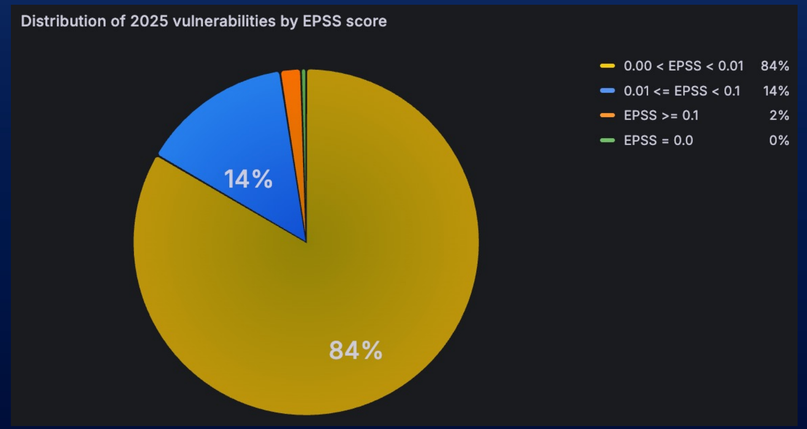
- Trojans and in particular Remote Access Trojans (RATs) dominate the threat landscape in the ASEAN region
- In 1H 2026, APTs linked to **China, Russia** and **Iran** were the ones most active here

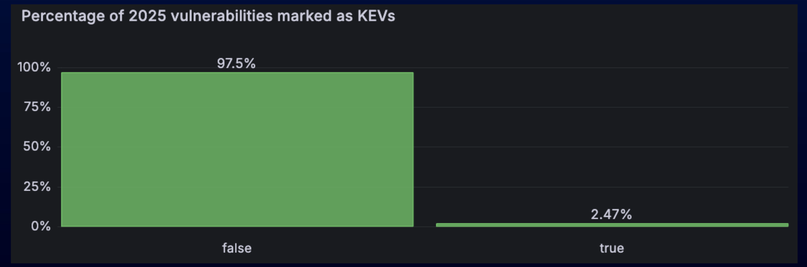
VULNERABILITY LANDSCAPE OF ASEAN COMPANIES

Top 5 recent OT vulnerabilities most commonly observed in ASEAN environments

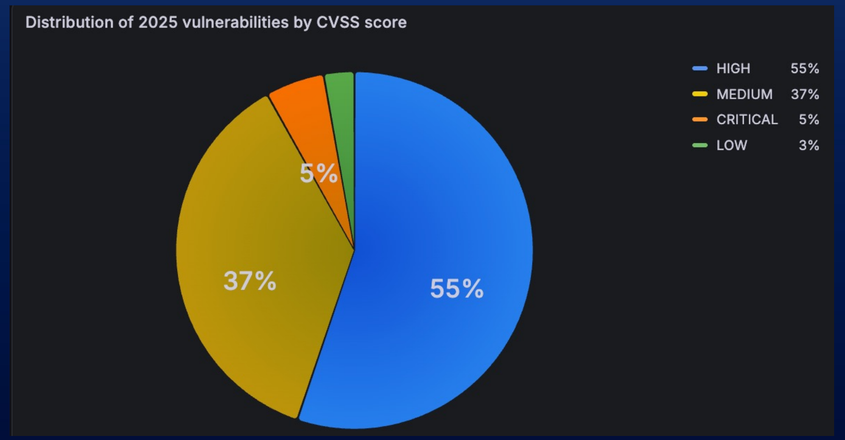
ID	CVSS	Product
CVE-2025-40833	**8.7**	Siemens (multiple devices)
CVE-2025-40943	**9.4**	Siemens SIMATIC S7-1500 devices
CVE-2025-7353	**9.3**	Rockwell Automation ControlLogix® Ethernet
CVE-2025-15467	**8.8**	OpenSSL (multiple versions)
CVE-2025-6625	**7.5**	Schneider Electric Modicon M340 and Communication Modules

- **Siemens**, **Rockwell Automation** and **Schneider Electric** are top affected OT vendors
- EPSS and KEV are meaningful, but not comprehensive

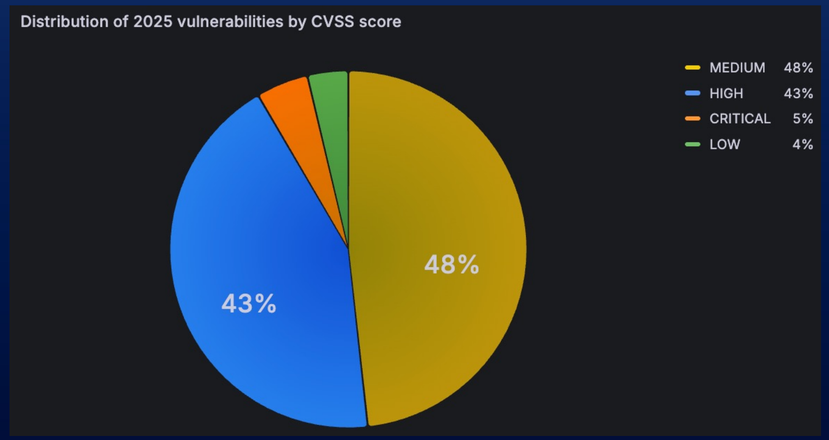




VULNERABILITY LANDSCAPE OF ASEAN COMPANIES



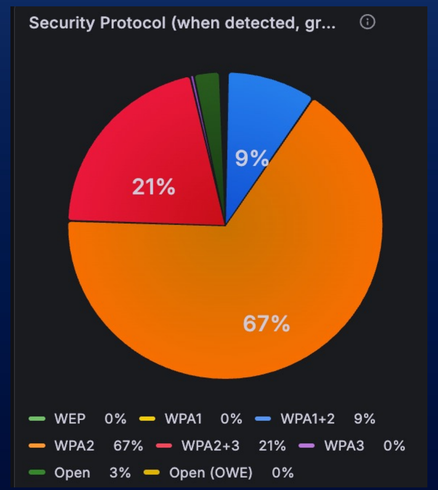
ASEAN region in 1H 2026

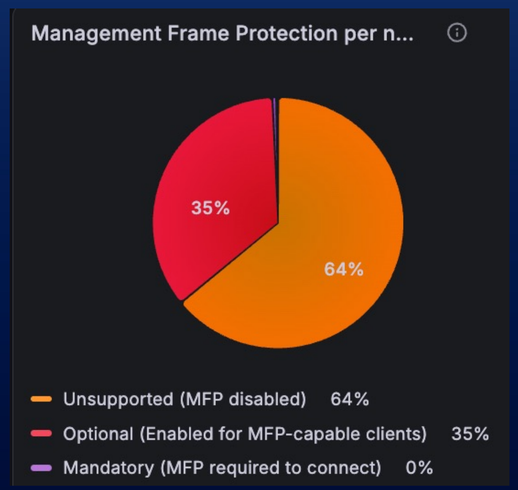


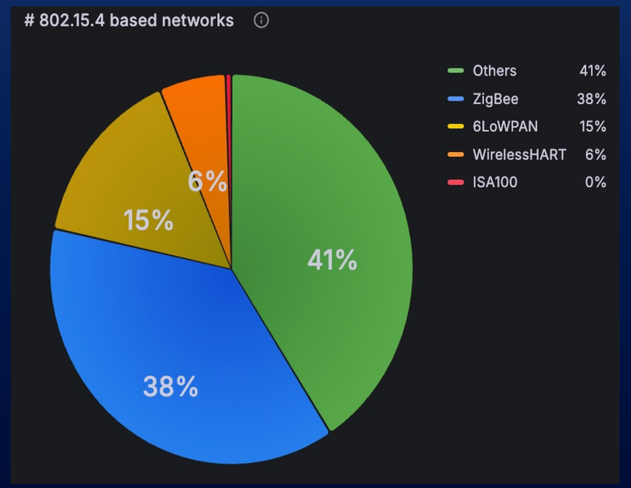
Global average in 1H 2026

- The proportion of recently discovered vulnerabilities with a **HIGH** CVSS score is **significantly higher** in the ASEAN region compared to the global average
- All the most prevalent recently discovered vulnerabilities have **HIGH** and **CRITICAL** CVSS scores

WIRELESS THREATS ACROSS THE GLOBE



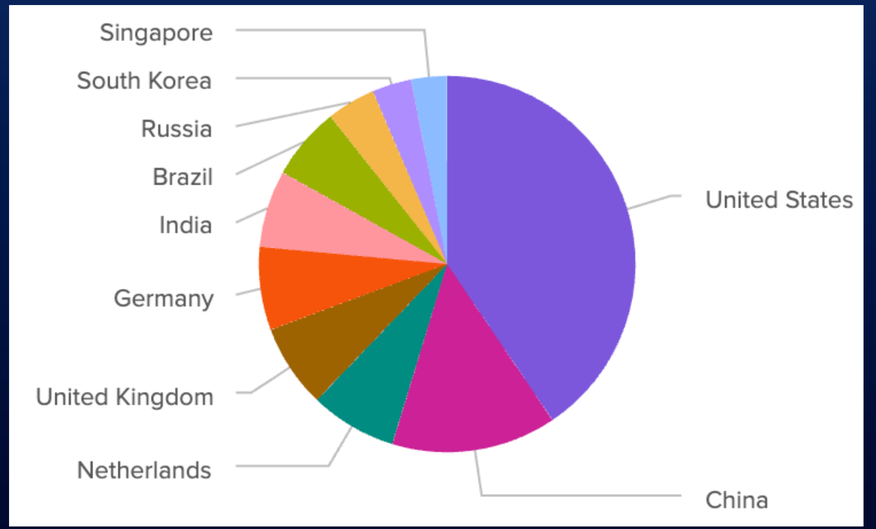




- In monitored Wi-Fi networks, WPA2 still remains the most commonly used security protocol
- MFP is still commonly not supported, allowing deauth attacks
- Zigbee, 6LoWPAN and WirelessHART are some of the most used 802.15.4 wireless protocols

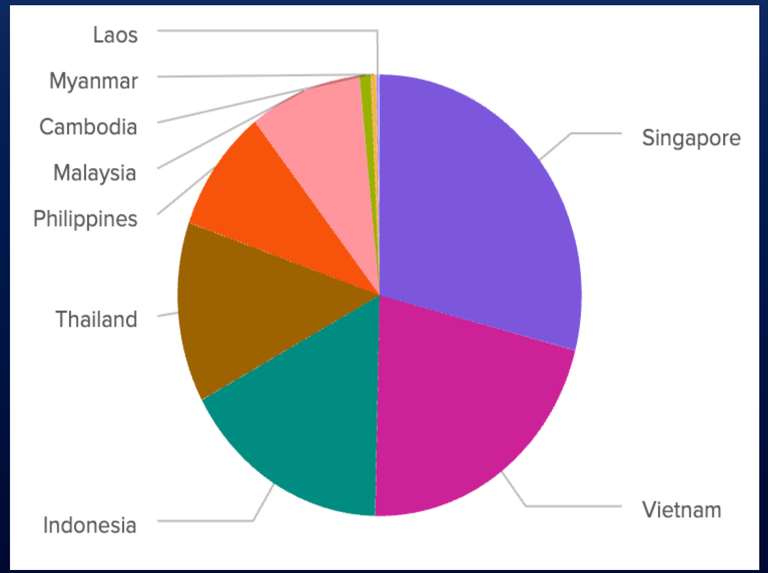
IOT BOTNET ACTIVITY IN ASEAN ENVIRONMENTS

- These botnet statistics are based on the number of unique IP addresses from which attacks against honeypots were originating
- In 1H 2026, most of the botnet attacks were originating from **the US**
- Compared to 2H 2025, the number of botnets located in **China** dropped significantly
- Another big change: **the Netherlands** went a few positions up taking 3rd place

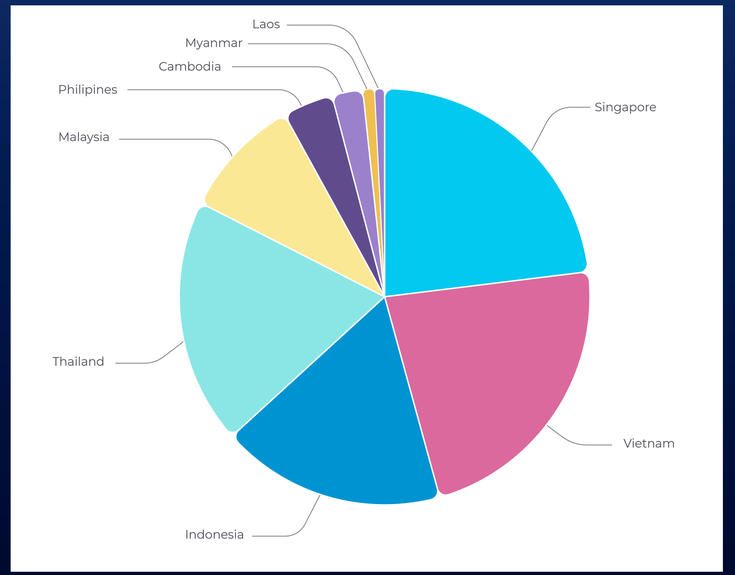


At the end of 1H 2026

IOT BOTNET ACTIVITY IN ASEAN ENVIRONMENTS



Botnets in the ASEAN region - 1H 2026



Botnets in the ASEAN region – 1H 2025

- In the ASEAN region, in 1H 2026, most of the botnet attacks were coming from **Singapore**
  - Their proportion has increased as well
- Compared to 1H 2025, the Philippines moved one position up overtaking Malaysia

ACTIONABLE RECOMMENDATIONS

- Establish complete **asset and network visibility** across OT and IoT
  - Including wired and wireless networks and endpoints

- Leverage **AI-driven** security systems to detect anomalies and threats

- Ensure **continuously updated** malware **prevention** for ICS networks

- Prioritize **risk-based** vulnerability management for OT environments

- Participate in **intelligence sharing** to improve collective cyber resilience

WE ARE STRONGER
TOGETHER!