NCSA สกมช
ThaiCERT
Thailand Computer Emergency Response Team
By NCSA Thailand

# HEALTHCARE TECHNOLOGY SUMMIT 2026

# FROM CYBERSECURITY READINESS TO HEALTHCARE RESILIENCY

**Wednesday, 23 September 2026, 13:20 - 13:50**

Mayfair Grand Ballroom, 11 Floor, The Berkeley Hotel Pratunam, Bangkok


**Air Vice Marshal Jadet Khuhakongkit**
**Assistant Secretary General**

PEOPLE
DATA
INFRASTRUCTURE
A SAFER TOMORROW

CYBER
INSIGHTS
FOR A SAFER
TOMORROW

GLOBAL
THREATS
REAL IMPACT
STRONGER
TOGETHER

A MORE
RESILIENT
WORLD

# GLOBAL CYBER THREAT LANDSCAPE 2026

## Healthcare is Among the World's Most Targeted Sectors

ภาพรวมอุตสาหกรรมที่ถูกโจมตีทางไซเบอร์มากที่สุดของโลก

**#1** Education
**4,352** attacks / organization / week

**#2** Government
**2,683** attacks / organization / week

**#3** Telecommunications
**2,656** attacks / organization / week

**#4** Healthcare & Medical
**2,365** attacks / organization / week

**#5** Energy & Utilities
**2,168** attacks / organization / week

### Healthcare in 2026

- #1 in GenAI sensitive data exposure risk (Aug 2026)
- #5 among ransomware victim industries in Aug 2026 (7%)

Healthcare & Medical ranks **#4** globally in cyber attacks per organization/week

Global average across industries: **1,968** attacks / organization / week

หมายเหตุ: ตัวเลขอันดับอุตสาหกรรมเป็นข้อมูลภาพรวมจากรายงาน Cyber Security Report 2026 และข้อมูลเสริมภาคสาธารณสุขจากรายงานเดือนสิงหาคม 2026

**References**


Check Point Research — Cyber Security Report 2026
Check Point Blog — The Trends Defining Cyber Security in 2026: Cyber Security Report 2026
Check Point Blog — August 2026 Cyber Threat Landscape: GenAI Data Exposure Emerges as a New Enterprise Risk as Attacks, Phishing, and Ransomware Accelerate

PEOPLE
DATA
INFRASTRUCTURE
A SAFER
TOMORROW

# 2026 Global Health Sector Threat Landscape

## ภาพรวมภัยคุกคามไซเบอร์ภาคสุขภาพ ปี 2026

Health-ISAC | January 2026 | TLP:WHITE

GLOBAL HEALTH
STRONGER
TOGETHER

*ความมั่นคงทางไซเบอร์*
*คือรากฐานของระบบสุขภาพที่ยั่งยืน*

HEALTHY SYSTEMS
SAFER COMMUNITIES
BRIGHTER TOMORROW

### รายงานนี้กล่าวถึงอะไร

รายงานฉบับนี้สรุปภัยคุกคามไซเบอร์ที่สำคัญต่อระบบสุขภาพทั่วโลก โดยอ้างอิงเหตุการณ์จริงในปี 2025 เพื่อเตรียมความพร้อมสู่ปี 2026

- ภัยคุกคามมีปริมาณมากขึ้น ซับซ้อนขึ้น และส่งผลเป็นวงกว้าง
- ภาคสุขภาพยังคงเป็นเป้าหมายสำคัญของอาชญากรไซเบอร์และรัฐชาติ
- ความเสี่ยงไม่ได้กระทบแค่ข้อมูล แต่รวมถึงการให้บริการและความปลอดภัยของผู้ป่วย

### ประเด็นสำคัญจากรายงาน

- **Ransomware**
- **Supply Chain Risk**
- **Social Engineering**
- **Business Resilience**

ประเด็นเด่นของปี 2025–2026 คือการโจมตีเรียกค่าไถ่ ความเสี่ยงจากคู่ค้า เทคนิคหลอกลวงผู้ใช้ และการสร้างความยืดหยุ่นขององค์กร

### ผลสำรวจผู้เชี่ยวชาญเกือบ 250 คน

**ความกังวลหลักในปี 2025**

1. Ransomware Deployments
2. Phishing Attacks
3. Third Party / Partner Breaches
4. Data Breaches
5. Zero-Day Exploits

**แนวโน้มความเสี่ยงในปี 2026**

1. AI-Enabled Attacks
2. Ransomware Deployments
3. Third Party Breaches
4. Zero-Day Exploits
5. Phishing / Spear Phishing

### โครงสร้างเนื้อหารายงาน

**Part I: Current Threat Landscape**
- Physical Security
- Cybercriminal Activity
- Nation-State Activity
- Medical Device Cybersecurity

**Part II: Tactics, Techniques and Procedures**
- ClickFix / FileFix
- QR Phishing
- Malware
- Notable Vulnerabilities

**Part III: Future Cybersecurity Outlook**
- Business Resilience
- Supply Chain Risk
- AI Governance
- Operational Continuity


SECURE
HEALTHCARE
BRIGHTER
LIVES

CONNECTED
DEFENDED
RESILIENT
FOR BETTER CARE

### ข้อความสำคัญที่รายงานต้องการสื่อ

1. Ransomware ยังคงเป็นภัยหลักของภาคสุขภาพ
2. ความมั่นคงปลอดภัยขององค์กรแข็งแรงได้เท่ากับจุดอ่อนของคู่ค้าและซัพพลายเชน
3. ปี 2026 ต้องขยับจากการตอบสนองเหตุการณ์ไปสู่การเสริมสร้าง Business Resilience

Source: Health-ISAC, 2026 Global Health Sector Threat Landscape

NCSA สกมช
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

Change Healthcare
A UnitedHealth Group Company

# CASE 01 CHANGE HEALTHCARE
## การโจมตีหลายแวร์กระทบต่อภาคธุรกิจสุขภาพในสหรัฐฯ

เหตุการณ์จริง | บทเรียนจริง | สังคมดิจิทัลที่ปลอดภัยกว่าเดิม

"ความปลอดภัยข้อมูลสุขภาพ คือความเชื่อมั่นของประชาชน การรักษาความปลอดภัยไซเบอร์"
PROTECT HEALTH DATA
PROTECT PEOPLE


"ข้อมูลสุขภาพไม่ใช้แค่ตัวเลข แต่คือชีวิตของผู้คน"


## 1 INCIDENT OVERVIEW

ในเดือนกุมภาพันธ์ 2024 บริษัท Change Healthcare ซึ่งเป็นบริษัทในเครือของ UnitedHealth Group และเป็นตัวกลางสำคัญของระบบธุรกรรมและการประมวลผลการเคลมด้านสุขภาพในสหรัฐอเมริกา ถูกกลุ่มแรนซัมแวร์ ALPHV/BlackCat โจมตี ส่งผลให้ระบบหยุดชะงักและกระทบต่อบริการสุขภาพในวงกว้าง

- **ก.พ. 2024** เกิดเหตุโจมตี
- Change Healthcare (UnitedHealth Group) ตัวกลางประมวลผลการเคลม
- **ALPHV/BlackCat** กลุ่มแรนซัมแวร์

## 2 ATTACK FLOW

1. ขโมยข้อมูลบัญชีผู้ใช้ (Credentials)
2. เข้าถึงระบบจากภายนอกโดยไม่ผ่าน MFA (VPN / Remote Access)
3. เข้าสู่ระบบและเคลื่อนไหวภายในเครือข่าย
4. ขโมยข้อมูลจำนวนมากออกจากระบบ (Data Exfiltration)
5. ติดตั้งแรนซัมแวร์ ทำให้ระบบหยุดชะงัก (Ransomware / Service Disruption)

## 3 DATA EXPOSED

**192.7 ล้านคน**
ได้รับผลกระทบ

### ข้อมูลที่ถูกเปิดเผย

- **ข้อมูลทางการแพทย์** เช่น ประวัติการรักษา ผลการตรวจ
- **ข้อมูลส่วนบุคคล** เช่น ชื่อ ที่อยู่ วันเกิด หมายเลขประกันสังคม (SSN)
- **ข้อมูลประกันสุขภาพ** เช่น ข้อมูลกรมธรรม์และการเคลม
- **ข้อมูลทางการเงิน** เช่น ข้อมูลการชำระเงินและบัญชีธนาคาร

### ผลกระทบสำคัญ

- กระทบต่อผู้ป่วย **192.7 ล้านคน** ซึ่งเป็นหนึ่งในการรั่วไหลข้อมูลสุขภาพที่ใหญ่ที่สุดในประวัติศาสตร์สหรัฐฯ
- ความเสียหายทางการเงิน **มากกว่า 3 พันล้านดอลลาร์สหรัฐ**
- ระบบบริการสุขภาพทั่วสหรัฐฯ หยุดชะงัก ส่งผลต่อโรงพยาบาล แพทย์ และผู้ป่วย

## 4 ROOT CAUSE

**Credential Leak + ไม่ได้เปิดใช้ MFA**

กลุ่มผู้โจมตีใช้ข้อมูลบัญชีผู้ใช้ที่ถูกจโมย (เก็บมาจากแหล่งภายนอก) เข้าถึงระบบจากภายนอก โดยที่ไม่มีการยืนยันตัวตนแบบหลายปัจจัย (MFA) ทำให้สามารถเข้าสู่ระบบและเคลื่อนไหวภายในได้

## 5 IMMEDIATE RESPONSE

- [x] แยกและควบคุมระบบที่ได้รับผลกระทบ (Isolate / Contain)
- [x] รีเซ็ตรหัสผ่านและปิดบัญชีที่มีความเสี่ยง
- [x] เปิดใช้งาน MFA ในทุกระบบ โดยเฉพาะการเข้าถึงจากภายนอก
- [x] แจ้งหน่วยงานที่เกี่ยวข้องและลูกค้า/ผู้รับบริการ
- [x] กู้คืนระบบและทยอยกลับมาให้บริการอย่างปลอดภัย


แหล่งอ้างอิง
1 Reuters (2024). Hack of UnitedHealth's tech unit impacted 192.7 million people, US health dept. website. https://www.reuters.com/business/healthcare-pharmaceuticals/hack-unitedhealths-tech-unit-impacted-1927-million-people-2025-08-14/
2 CNA (2024). UnitedHealth Group paid over $3 billion to providers since cyberattack. https://www.channelnewsasia.com/business/unitedhealth-group-cyberattack-change-healthcare-5186901


TOGETHER FOR A SAFER HEALTHCARE SYSTEM

NCSA สกมช
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

# CASE 02 Synnovis / NHS London Ransomware Attack

โจมตีระบบห้องปฏิบัติการ กระทบการตรวจเลือดและการรักษาผู้ป่วยในกรุงลอนดอน

REAL INCIDENT | REAL LESSONS | A SAFER THAILAND

"Cybersecurity in Healthcare is Patient Safety"

SAFE, SECURE, & TRUSTED CYBERSPACE FOR THAILAND

NHS


กระทบโรงพยาบาลหลายแห่งในกรุงลอนดอน สหราชอาณาจักร

"ระบบสาธารณสุขที่มั่นคง คือรากฐานของสังคมที่ปลอดภัย"

PEOPLE | PROCESS | TECHNOLOGY | COOPERATION | RESILIENCE

## 1 INCIDENT OVERVIEW

**วันที่ 3 มิถุนายน 2567**
(3 June 2024)

Synnovis ผู้ให้บริการตรวจทางห้องปฏิบัติการแก่ NHS ในกรุงลอนดอน ถูกโจมตีด้วย Ransomware ทำให้ระบบ IT ของห้องปฏิบัติการได้รับผลกระทบอย่างรุนแรง ส่งผลให้การตรวจเลือดและการให้บริการผู้ป่วยล่าช้าในวงกว้าง

| NHS | > 11,000 | บริการกลับสู่ปกติ |
|---|---|---|
| หลายโรงพยาบาลในกรุงลอนดอน | นัดหมาย/หัตถการที่ถูกเลื่อนหรือยกเลิก | ถึงเดือน 2567 (Dec 2024) |

## 2 ATTACK FLOW

กลุ่ม Qilin Ransomware → เข้าระบบของ Synnovis → ระบบห้องปฏิบัติการไม่สามารถใช้งานได้ → ขโมยข้อมูล (Data Theft) → ข่มขู่ข้อมูลออกเผยแพร่บนเว็บไซต์ของกลุ่มผู้โจมตี

## 3 IMPACT / DATA EXPOSED

| การตรวจเลือดและ Pathology ได้รับผลกระทบ | > 11,000 นัดหมาย/หัตถการถูกเลื่อนหรือยกเลิก | ต้องใช้กระบวนการแบบ Manual ในหลายส่วน | มีข้อมูลถูกขโมยและบางส่วนเผยแพร่ 20 มิถุนายน 2567 |
|---|---|---|---|

## 4 ROOT CAUSE

**Ransomware (Qilin)**

การโจมตีถูกเชื่อมโยงกับกลุ่ม Qilin ransomware อย่างไรก็ตาม รายละเอียดวิธีการเข้าระบบครั้งแรกยังไม่ได้รับการเปิดเผยอย่างชัดเจน

## 5 RESPONSE

- ✓ ใช้ระบบ Manual ชั่วคราว และกระจายงานตรวจไปยังห้องปฏิบัติการอื่น
- ✓ สร้างระบบ IT ใหม่ (Rebuild > 60 ระบบ)
- ✓ ทำงานร่วมกับ NHS England, NCSC และ NCA
- ✓ ระบบต่าง ๆ กลับมาให้บริการได้ครบในเดือน ธ.ค. 2567

**The Guardian**

**Russian group behind London hospitals cyber-attack says expert**

*July 5, 2024*

https://www.theguardian.com/technology/article/2024/jun/05/russian-group-behind-london-hospitals-cyber-attack-says-expert

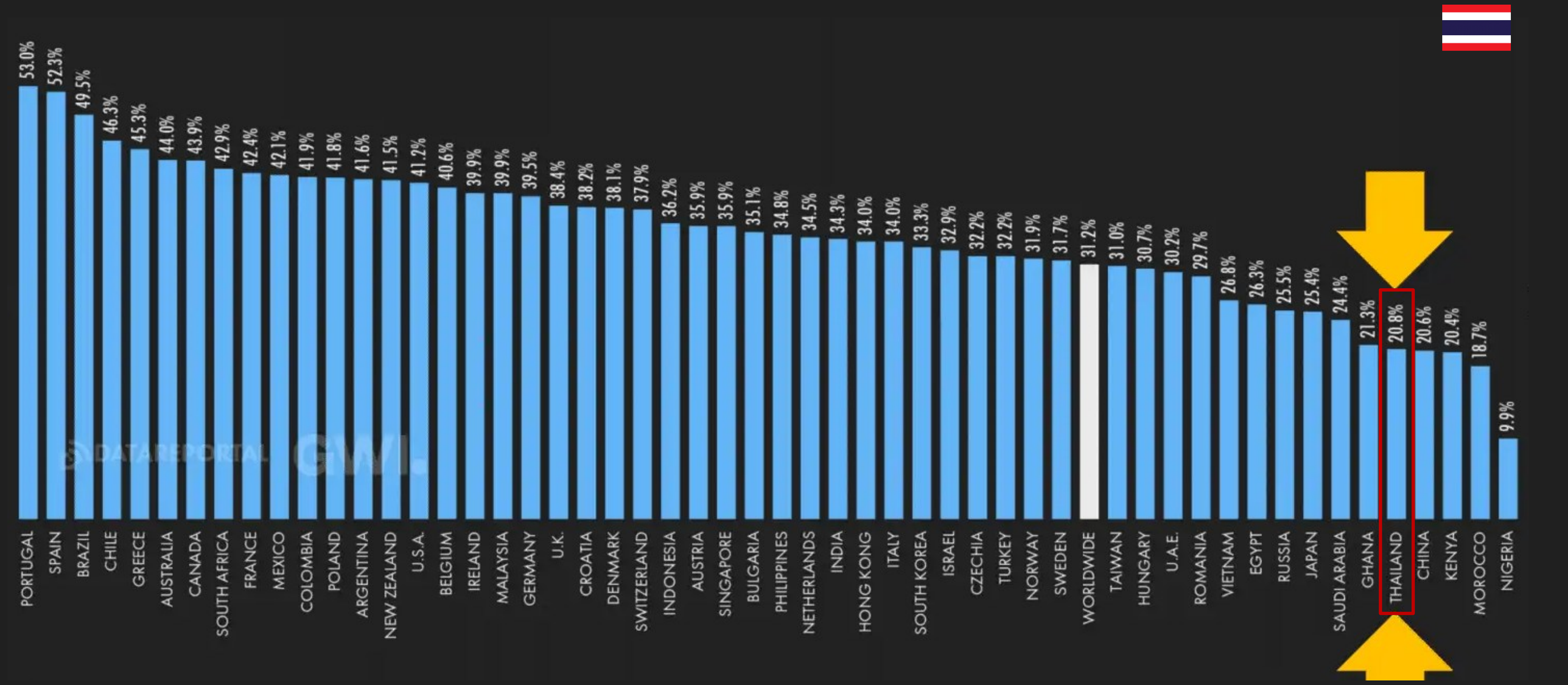
**NHS England**

**Synnovis cyber incident**

3 June 2024


https://www.england.nhs.uk/synnovis-cyber-incident/

# คนไทยกังวลเรื่องข้อมูลส่วนบุคคลหลุดแค่ 20.8% เท่านั้น




https://datareportal.com/reports/digital-2024-thailand

# ไทย ติด 1 ใน 10 ประเทศที่มีข้อมูลรั่วไหลบนดาร์กเว็บมากที่สุด



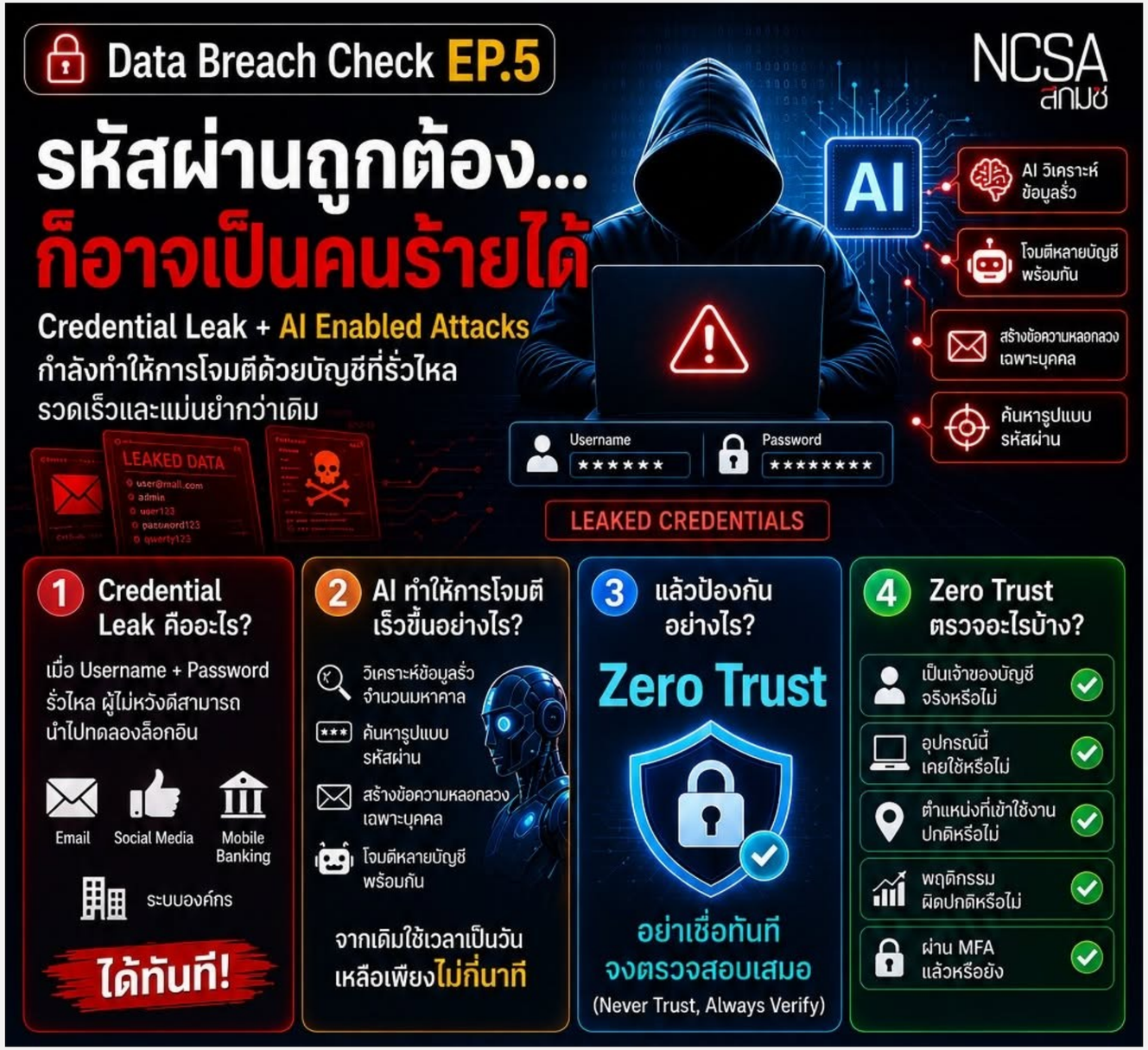
ไทย ติด 1 ใน 10 ประเทศที่มีข้อมูลรั่วไหลบนดาร์กเว็บมากที่สุด
รายงาน High-Tech Crime Trends โดย Group-IB พบว่าปี 2024 พบข้อมูลรั่วไหลสู่สาธารณะ 1,107 เคสทั่วโลก ทำให้ข้อมูลผู้ใช้มากกว่า 6.4 พันล้านรายการถูกบุกรุก โดยในบรรดาข้อมูลที่รั่วไหล อีเมล หมายเลขโทรศัพท์ และรหัสผ่านมีความเสี่ยงสูงสุด เนื่องจากผู้คุกคามสามารถใช้ข้อมูลตรงนี้โจมตีได้
จากข้อมูลที่รั่วไหลทั้งหมด กว่า 6.5 พันล้านรายการ เป็นข้อมูลที่มีอีเมลเป็นส่วนประกอบ ในขณะที่ 3.3 พันล้านรายการมีหมายเลขโทรศัพท์เป็นส่วนประกอบ และรหัสผ่านที่ถูกเปิดเผยกว่า 460 ล้านรายการ

.

ซึ่งอินโดนีเซีย และไทย ติด 1 ใน 10 ตลาดทั่วโลกที่ได้รับผลกระทบจากการรั่วไหลของข้อมูลบนดาร์กเว็บมากที่สุด

https://www.facebook.com/blognone/posts/pfbid0sZkZUirixNiCrSaNe1AfY625MWqLc18k6BR5CJB66mGNGgRT2C71wDbbvtg5Asgwl?rdid=ZrJHRGak5eOgdbRq#

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

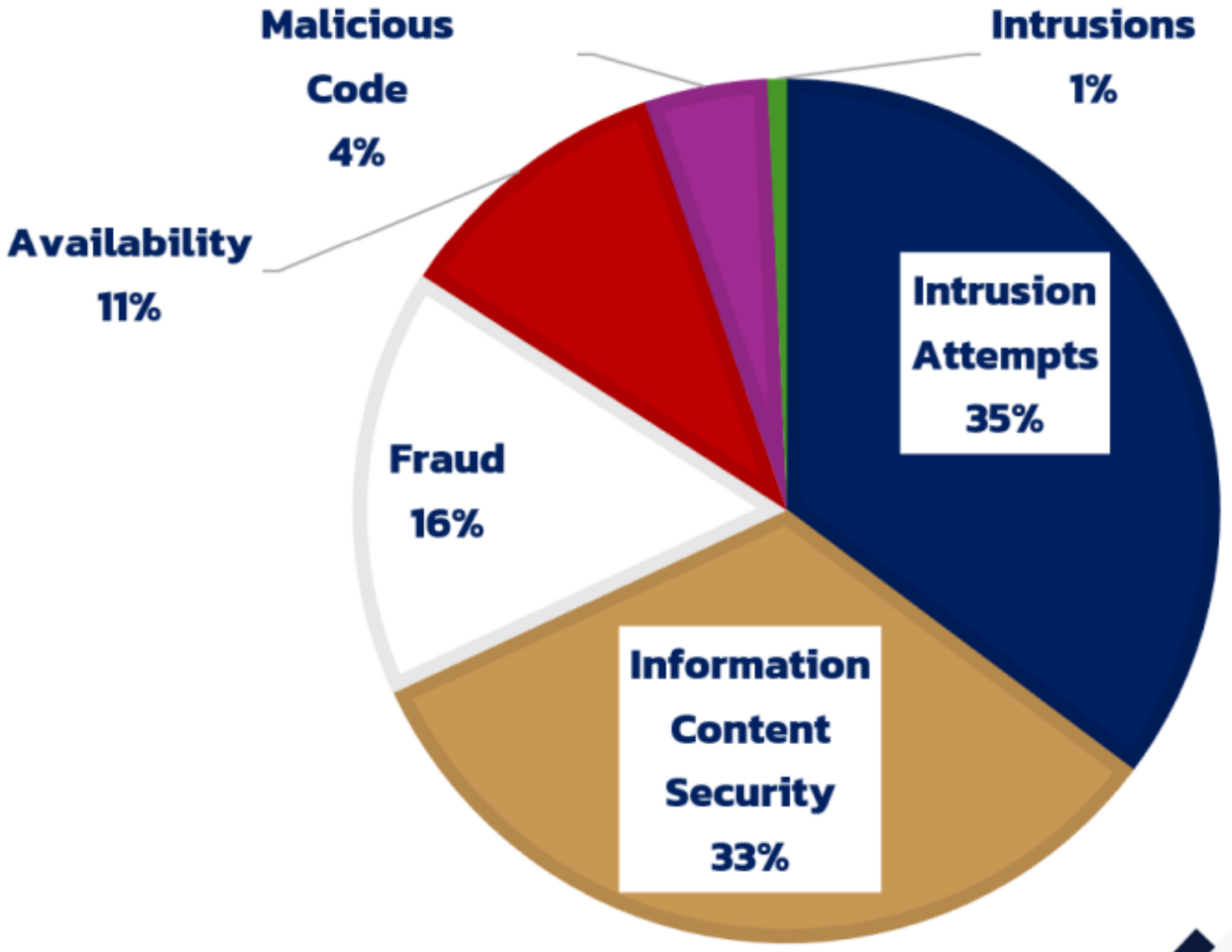



# สถิติภัยคุกคามทางไซเบอร์ ประจำปี พ.ศ. 2569

## มกราคม 2569 – สิงหาคม 2569

### รวมทั้งสิ้น 2,986 เหตุการณ์

| | |
|---|---|
| Intrusion Attempts | 1,052 |
| Information Content Security | 981 |
| Fraud | 478 |
| Availability | 317 |
| Malicious Code | 137 |
| Intrusions | 21 |

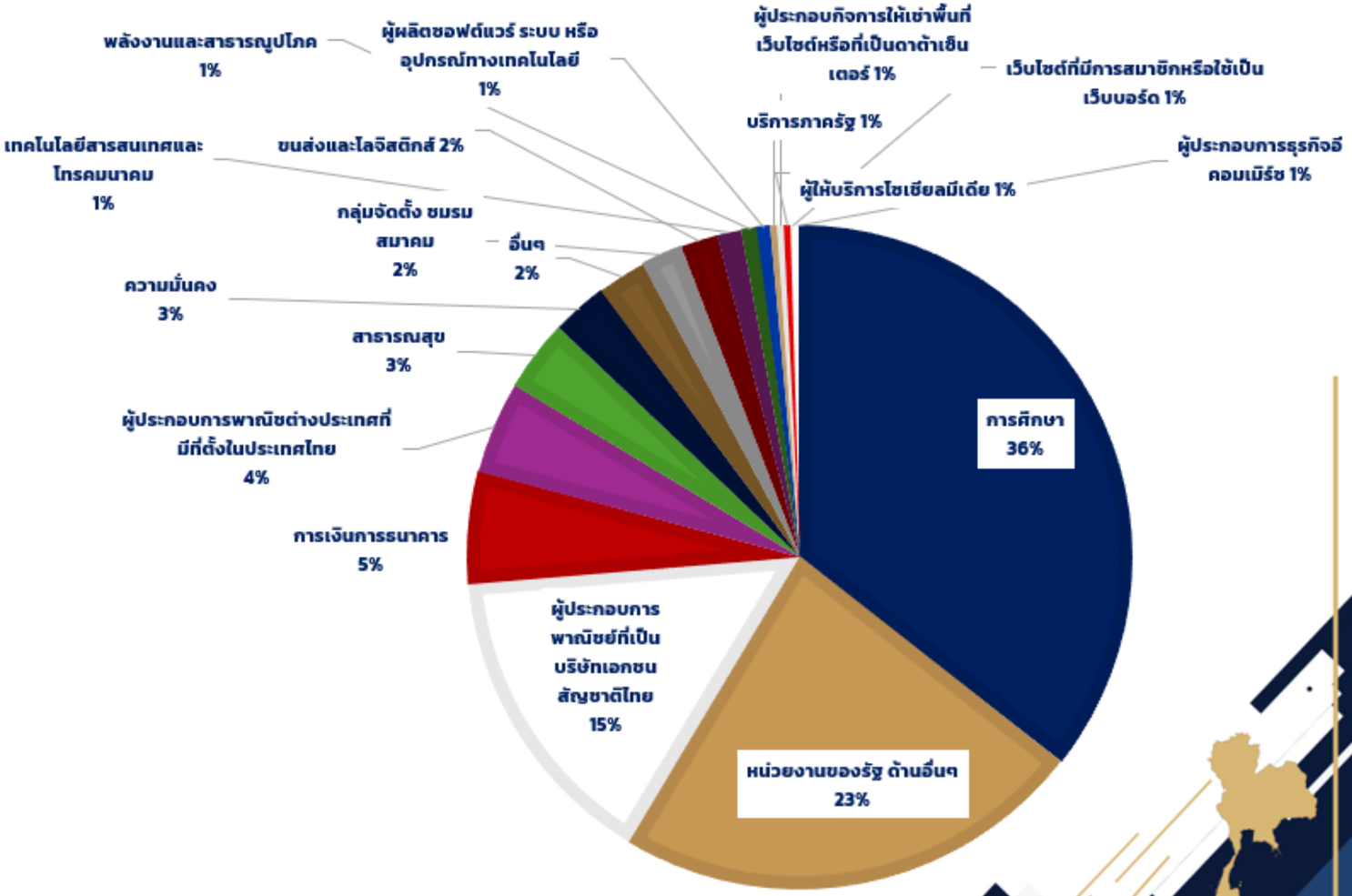


# สถิติภัยคุกคามทางไซเบอร์ ประจำปี พ.ศ. 2569

## มกราคม 2569 – สิงหาคม 2569

### รวมทั้งสิ้น 2,986 เหตุการณ์

| | |
|---|---|
| การศึกษา | 1,062 |
| หน่วยงานของรัฐ ด้านอื่นๆ | 688 |
| ผู้ประกอบการพาณิชย์ที่เป็นบริษัทเอกชน สัญชาติไทย | 451 |
| การเงินการธนาคาร | 162 |
| ผู้ประกอบการพาณิชต่างประเทศที่มีที่ตั้งในประเทศไทย | 134 |
| สาธารณสุข | 94 |
| ความมั่นคง | 81 |
| อื่นๆ | 71 |
| กลุ่มจัดตั้ง ชมรม สมาคม | 60 |
| ขนส่งและโลจิสติกส์ | 54 |
| เทคโนโลยีสารสนเทศและโทรคมนาคม | 35 |
| พลังงานและสาธารณูปโภค | 24 |
| ผู้ผลิตซอฟต์แวร์ ระบบ หรืออุปกรณ์ทางเทคโนโลยี | 19 |
| บริการภาครัฐ | 10 |
| ผู้ประกอบกิจการให้เช่าพื้นที่เว็บไซต์หรือที่เป็นดาต้าเซ็นเตอร์ | 9 |
| ผู้ให้บริการโซเชียลมีเดีย | 9 |
| เว็บไซต์ที่มีการสมาชิกหรือใช้เป็นเว็บบอร์ด | 7 |
| ผู้ประกอบการธุรกิจอีคอมเมิร์ซ | 6 |




SAFE, SECURE, & TRUSTED CYBERSPACE FOR THAILAND

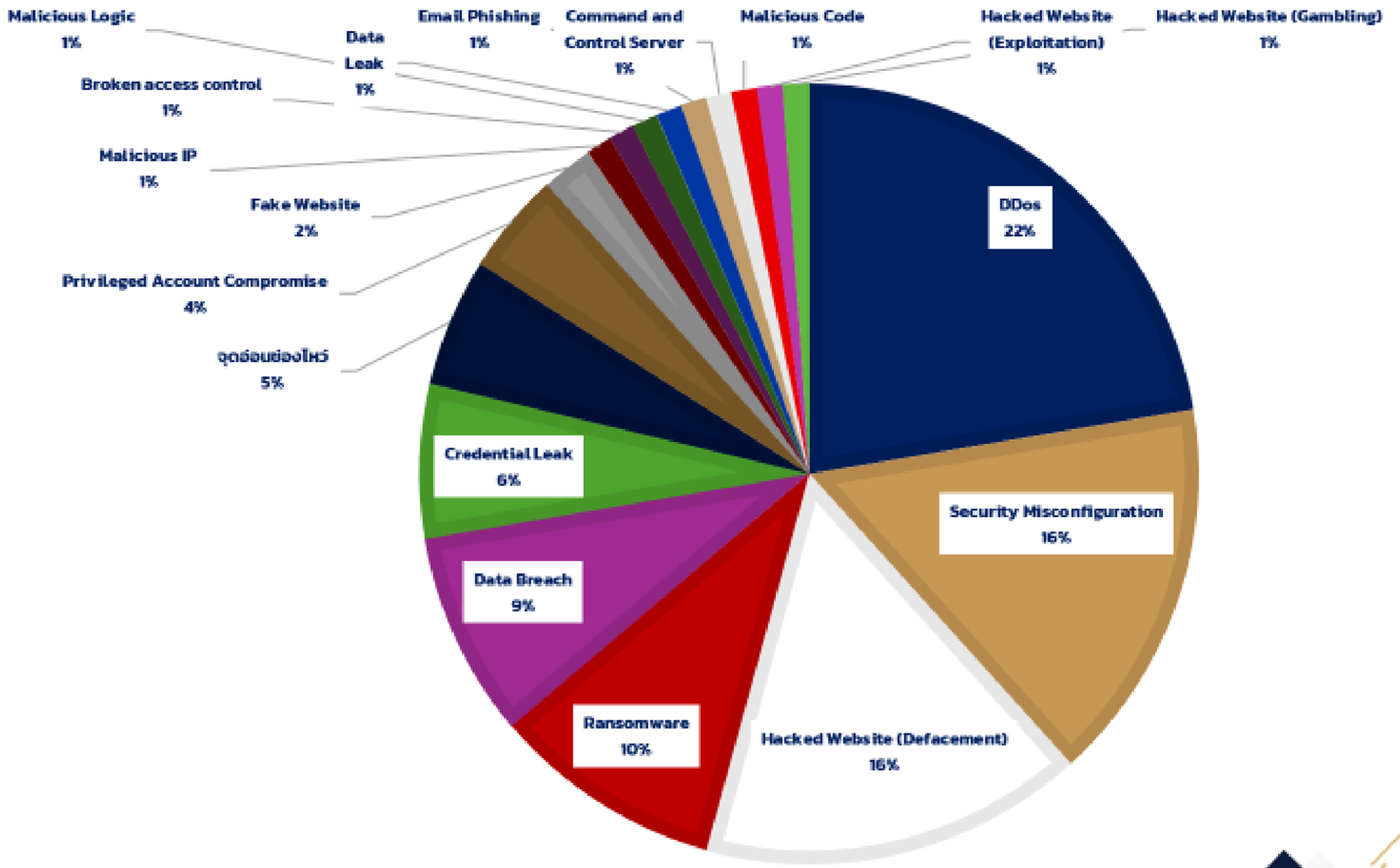
# สถิติภัยคุกคามทางไซเบอร์ ประจำปี พ.ศ. 2569

## มกราคม 2569 – สิงหาคม 2569

## หน่วยงานสาธารณสุข

### รวมทั้งสิ้น 94 เหตุการณ์

| | |
|---|---|
| DDos | 21 |
| Security Misconfiguration | 15 |
| Hacked Website (Defacement) | 15 |
| Ransomware | 9 |
| Data Breach | 8 |
| Credential Leak | 6 |
| จุดอ่อนช่องโหว่ | 5 |
| Privileged Account Compromise | 4 |
| Fake Website | 2 |
| Malicious IP | 1 |
| Broken access control | 1 |
| Malicious Logic | 1 |
| Data Leak | 1 |
| Email Phishing | 1 |
| Command and Control Server | 1 |
| Malicious Code | 1 |
| Hacked Website (Exploitation) | 1 |
| Hacked Website (Gambling) | 1 |



NCSA สกมช.

ThaiCERT
Thailand Computer Emergency Response Team
By NCSA Thailand

# CASE 01 DATA BREACH
## การรั่วไหลและประกาศขายข้อมูลในระบบทางการแพทย์

REAL INCIDENT | REAL LESSONS | A SAFER THAILAND

SAFE, SECURE, & TRUSTED CYBERSPACE FOR THAILAND

"ร่วมปกป้องประเทศ จากภัยคุกคามทางไซเบอร์"


"ข้อมูลของประชาชนคือความไว้วางใจ เราพร้อมปกป้อง และตอบสนองอย่างรวดเร็ว"


## 1 INCIDENT OVERVIEW

ตรวจพบการประกาศขายข้อมูลของระบบทางการแพทย์ บนเว็บไซต์ BreachForums ในราคา 6,000 ดอลลาร์สหรัฐ (ประมาณ 202,506 บาท)

| วันที่ตรวจพบ | จำนวนข้อมูล | ราคาขาย |
|---|---|---|
| 12 มีนาคม 2568 เวลา 09:20 น. | 3,197,083 รายการ | USD 6,000 (~202,506 บาท) |

## EVIDENCE : BREACHFORUMS POST

Thailand Medical Database - 3,197,083 Records
โดย Unknown
Posted: Mar 12, 2025 09:20 AM

Thailand Medical Database
3,197,083 records
Price: $6,000
Sample: https://...

Sample Data (บางส่วน)

Download Sample

| username | fullname | phone | email | citizen_id |
|---|---|---|---|---|
| user001 | [redacted] | 08xxxxxxxx | xxx@xxxx.com | 1xxxxxxxxxxxx |
| user002 | [redacted] | 08xxxxxxxx | xxx@xxxx.com | 1xxxxxxxxxxxx |
| user003 | [redacted] | 08xxxxxxxx | xxx@xxxx.com | 1xxxxxxxxxxxx |
| user004 | [redacted] | 08xxxxxxxx | xxx@xxxx.com | 1xxxxxxxxxxxx |
| user005 | [redacted] | 08xxxxxxxx | xxx@xxxx.com | 1xxxxxxxxxxxx |

## 2 ATTACK FLOW


## 3 DATA EXPOSED
ข้อมูลที่ถูกอ้างว่ารั่วไหล

| ชื่อบัญชีผู้ใช้งาน (Username) | ชื่อ-นามสกุล (Full Name) | หมายเลขโทรศัพท์ (Phone) | อีเมล (Email) | เลขประจำตัวประชาชน (Citizen ID) |
|---|---|---|---|---|

## 4 ROOT CAUSE

**Credential Leak**

การรั่วไหลของข้อมูลบัญชีผู้ใช้งาน ทำให้ผู้ไม่หวังดีสามารถเข้าถึงระบบและดึงข้อมูลได้

## 5 IMMEDIATE RESPONSE

**ดำเนินการทำ MFA**

เพื่อป้องกันการเข้าถึงระบบด้วยบัญชีที่รั่วไหล

DETECT | ANALYZE | RESPOND | COORDINATE | PROTECT

TOGETHER, WE ARE ThaiCERT

NCSA สกมช
ThaiCERT
Thailand Computer Emergency Response Team
By NCSA Thailand

DETECT
ANALYZE
RESPOND
TOGETHER
FOR A SAFER THAILAND

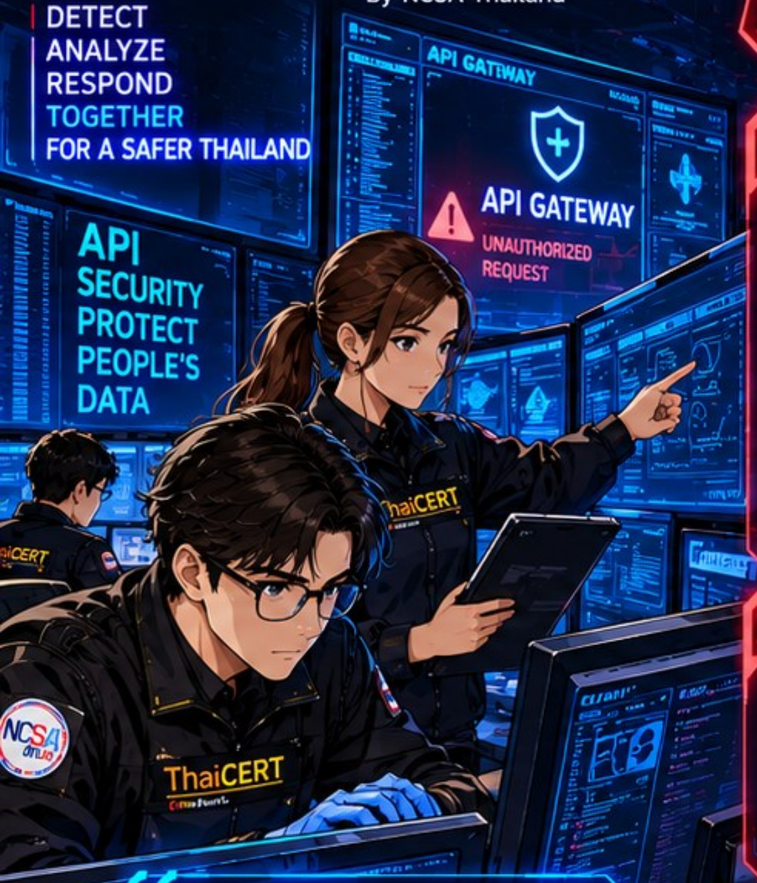
# CASE 02 API DATA EXPOSURE

## ช่องโหว่ API และบัญชีผู้ใช้งานรั่วไหลในระบบสุขภาพ

REAL INCIDENT | REAL LESSONS | A SAFER THAILAND

SAFE, SECURE, & TRUSTED CYBERSPACE FOR THAILAND

"ร่วมปกป้องประเทศ จากภัยคุกคามทางไซเบอร์"




"ข้อมูลสุขภาพของประชาชน
คือความไว้วางใจ
เราจะไม่ปล่อยให้รั่วไหลอีก"


ไซเบอร์ไทย
มั่นคง ปลอดภัย ไปด้วยกัน

## 1 INCIDENT OVERVIEW

**วันที่ 20 มีนาคม 2569 เวลา 09:00 น.**
ตรวจพบบัญชีผู้ใช้งานระบบสุขภาพเผยแพร่บนช่องทางภายนอก จำนวน 258,427 รายการ และมีการเผยแพร่ไฟล์บีบอัดขนาด 1.13 กิกะไบต์ ผ่านเว็บไซต์รับฝากไฟล์

| 258,427 | 1.13 GB | 20 มี.ค. 2569 |
|---|---|---|
| บัญชีผู้ใช้งานที่รั่วไหล | ไฟล์บีบอัดข้อมูลบนเว็บไซต์ภายนอก | เวลา 09:00 น. (ตรวจพบ) |

## EVIDENCE : LEAKED ACCOUNTS & API RESPONSE

ตัวอย่างบัญชีผู้ใช้งานที่รั่วไหล (บางส่วน)

| username | password |
|---|---|
| user1001 | ******* |
| user1002 | ******* |
| user1003 | ******* |
| user1004 | ******* |
| user1005 | ******* |
| ... | ... |

ตัวอย่างการเรียกใช้งาน API ที่ไม่ได้รับอนุญาต

Request | Response

```
{
  "cid": "1xxxxxxxxxxx",
  "fullname": "นายสมชาย ใจดี",
  "address": "123 หมู่ 1 ต. .....",
  "scheme": "สิทธิบัตรทอง",
  "hospital": "รพ. .....",
}
```

สามารถดึงข้อมูลส่วนบุคคลได้
- ชื่อ-นามสกุล
- เลขประจำตัวประชาชน
- ที่อยู่
- สิทธิการรักษาพยาบาล
- ไม่พบประวัติการรักษาพยาบาล

## 2 ATTACK FLOW

Leaked Accounts (บัญชีผู้ใช้งานรั่วไหล) → เชื่อมต่อและเรียกใช้งาน API โดยมีชอบ → ดึงข้อมูลส่วนบุคคลจากระบบสุขภาพ → 1.13 GB รวบรวมและบีบอัดข้อมูล → เผยแพร่บนเว็บไซต์รับฝากไฟล์ภายนอก → ข้อมูลรั่วไหลสู่สาธารณะ

## 3 DATA EXPOSED

ข้อมูลที่ถูกดึงออกไปจาก API

| ชื่อ-นามสกุล (Full Name) | เลขประจำตัวประชาชน (Citizen ID) | ที่อยู่ (Address) | สิทธิการรักษาพยาบาล (ข้าราชการ / ประกันสังคม / บัตรทอง) | ไม่พบข้อมูลประวัติการรักษาพยาบา |
|---|---|---|---|---|

## 4 ROOT CAUSE

**ไม่ได้ดำเนินการ API Security**

ขาดมาตรการป้องกันและควบคุมการเข้าถึง API อย่างเหมาะสม

## 5 RESPONSE

**ระงับการเข้าถึงและปิดกั้น API ทันที**

**ให้ดำเนินการ API Security**
- ตรวจสอบและเสริมความมั่นคง API
- ควบคุมการเข้าถึง (Authentication)
- ติดตามและเฝ้าระวังการใช้งาน (Monitoring)

PEOPLE | PROCESS | TECHNOLOGY | COOPERATION | RESILIENCE

TOGETHER, WE ARE ThaiCERT

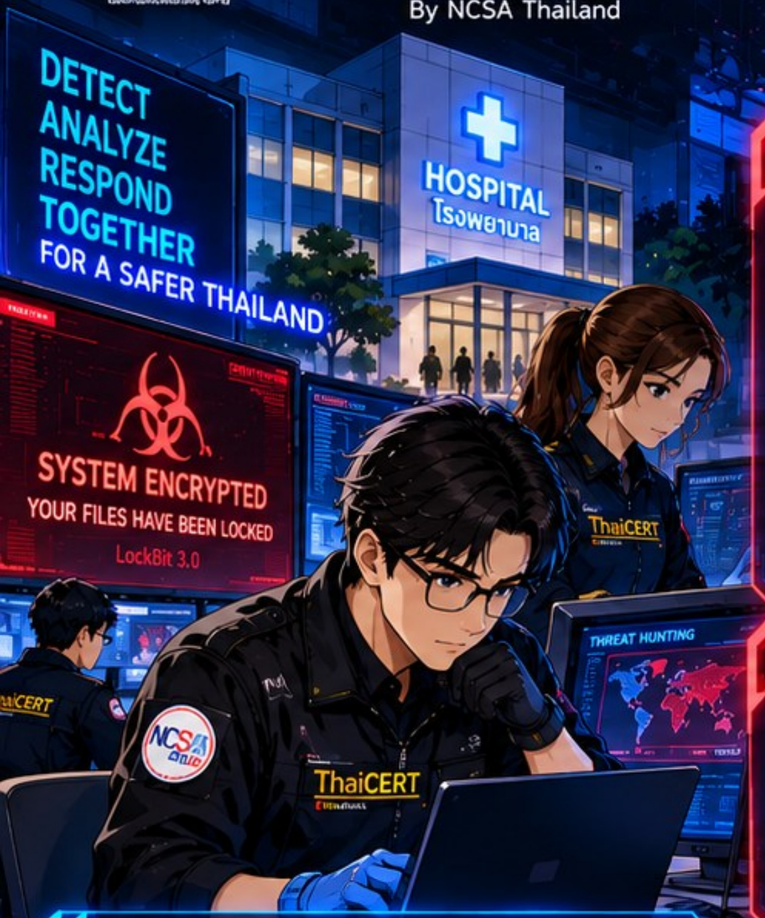
NCSA สกมช. | ThaiCERT Thailand Computer Emergency Response Team
By NCSA Thailand

# CASE 03 RANSOMWARE
## โรงพยาบาล ผ่าน AnyDesk

REAL INCIDENT | REAL LESSONS | A SAFER THAILAND

SAFE, SECURE, & TRUSTED CYBERSPACE FOR THAILAND

"ร่วมปกป้องประเทศ จากภัยคุกคามทางไซเบอร์"




"หยุดเหตุได้เร็ว ลดความเสียหายได้มาก ความร่วมมือคือเกราะป้องกันที่แข็งแกร่งที่สุด"


ไซเบอร์ไทย มั่นคง ปลอดภัย ไปด้วยกัน

## 1 INCIDENT OVERVIEW

**วันที่ 3 กันยายน 2569 เวลา 01:00 น.**

ผู้ไม่หวังดีเชื่อมต่อจาก IP 8.231.255.233 (Google Cloud) ผ่าน AnyDesk โดยใช้รหัสผ่าน Unattended Access และสั่งติดตั้ง Ransomware (LockBit 3.0)

| 8.231.255.233 | AnyDesk | ASX.exe | 3 ก.ย. 2569 |
|---|---|---|---|
| (Google Cloud) | (Unattended Access) | (LockBit 3.0) | 01:00 น. |

## EVIDENCE : ATTACKER ACTIVITY (จาก Log)

- เชื่อมต่อผ่าน AnyDesk จาก IP 8.231.255.233 (Google Cloud) โดยใช้รหัสผ่าน Unattended Access
- สแกนเครือข่ายด้วย Anonymous Logon 15,739 ครั้ง
- ปิด Windows Defender (Event ID 5001)
- ล้าง Security Log (Event ID 1102)
- ส่งไฟล์มัลแวร์ ASX.exe (LockBit 3.0) ผ่าน Clipboard ของ AnyDesk

ตัวอย่างเหตุการณ์ใน Log

```
8.231.255.233 - AnyDesk Connection Unattended Access
Anonymous Logon : 15,739 attempts
Event ID 5001 - Windows Defender stopped
Event ID 1102 - Security Log cleared
File Transfer : ASX.exe via Clipboard (AnyDesk)
Ransomware : LockBit 3.0
```

**SYSTEMS ENCRYPTED** LockBit 3.0

## 2 ATTACK FLOW

1. Threat Actor (8.231.255.233) Google Cloud
2. เชื่อมต่อผ่าน AnyDesk (Unattended Access)
3. สแกนเครือข่าย Anonymous Logon 15,739 ครั้ง
4. ปิด Windows Defender (Event ID 5001) ล้าง Security Log (Event ID 1102)
5. ส่ง ASX.exe (LockBit 3.0) ผ่าน Clipboard
6. แพร่กระจายภายในเครือข่ายห้องแล็บ (192.168.55.0/24)
7. เข้ารหัสข้อมูล Ransomware (LockBit 3.0)

## 3 IMPACT

- ระบบหยุดให้บริการ กระทบการดูแลผู้ป่วย
- ข้อมูลถูกเข้ารหัส ไม่สามารถใช้งานได้
- กระทบต่อการดำเนินงานของโรงพยาบาล

## 4 ROOT CAUSE

- ☑ Remote Access ที่ไม่มีการควบคุม
- ☑ เครือข่ายห้องแล็บเชื่อมตรงกับเซิร์ฟเวอร์ โดยไม่แบ่ง VLAN
- ☑ เครื่องปลายทางมีโปรแกรมละเมิดลิขสิทธิ์
- ☑ ไม่มีระบบ EDR

## 5 RESPONSE & PREVENTION

- ☑ Access control (ควบคุมการเข้าถึง)
- ☑ Zero Trust
- ☑ แยกเครือข่าย (Network Segmentation)
- ☑ ติดตั้ง EDR ในเครื่องปลายทาง
- ☑ เฝ้าระวังและตรวจจับพฤติกรรมผิดปกติ

PEOPLE | PROCESS | TECHNOLOGY | COOPERATION | RESILIENCE

TOGETHER, WE ARE ThaiCERT

ThaiCERT
Thailand Computer Emergency Response Team
By NCSA Thailand

NCSA สกมช

# ครม. เดินหน้า ยกระดับ MFA ทุกหน่วยงานรัฐ

เพิ่มเกราะป้องกันการสวมบัญชี
เมื่อ Username และ Password รั่วไหล

**Multi-Factor Authentication: MFA**
คือการยืนยันตัวตนมากกว่า 1 ขั้น
แม้รหัสผ่านรั่ว ผู้ไม่หวังดีก็เข้าใช้บัญชีได้ยากขึ้น

## แผนขับเคลื่อน 30–60–90 วัน

**ภายใน 30 วัน – สำรวจและจัดทำ Baseline**
- ยืนยันรายการระบบหรือ URL
- สำรวจระบบสำคัญและข้อมูลส่วนบุคคล
- รายงานสถานะ MFA และแผนปรับปรุง

**ภายใน 60 วัน – เร่งปรับปรุงระบบสำคัญ**
- เปิด MFA สำหรับ Admin / Privileged / Remote
- เร่งระบบบริการประชาชนและ Internet-facing
- กำหนดมาตรการทดแทนสำหรับระบบเดิม

**ภายใน 90 วัน – ขยายผลและวางมาตรฐานถาวร**
- ปิดช่องว่าง MFA ของระบบอื่นตามความเสี่ยง
- ใช้ Website Security Standard
- ใช้ Cloud Security Standard กับระบบ Cloud

## สิ่งที่ทุกหน่วยงานจะได้รับ

**ลดความเสี่ยง**
Force Reset Password
และปิดระบบ/ลบข้อมูล หากไม่ใช้

**เพิ่มความมั่นใจ**
ระบบปลอดภัย
เชื่อถือได้

**พร้อมปฏิบัติตามนโยบาย**
สอดคล้องกับมาตรฐาน
และข้อกำหนดภาครัฐ

> “ MFA ไม่ใช่การเพิ่ม แต่คือเกราะที่ทำให้องค์กรไทย **มั่นคง ปลอดภัย และเชื่อถือได้** ”

---

กมช. ผนึกกำลังทุกกระทรวง

# ยกระดับความมั่นคงปลอดภัยไซเบอร์ ด้วย MFA เร่ง Reset Password

พร้อมแผนสำรวจรัฐ/เอกชน
ขับเคลื่อนเตรียมประเทศไทยเปลี่ยนผ่านสู่
**Post-Quantum Cryptography (PQC)**

NCSA สกมช

**มุ่งลดความเสี่ยงจาก Credential รั่วไหล**
ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
คุ้มครองข้อมูลส่วนบุคคลและข้อมูลสำคัญของภาครัฐ

**หัวใจสำคัญ**
เร่งนำ Multi-Factor Authentication (MFA)
มาใช้กับระบบสารสนเทศภาครัฐ

**ระบบที่ให้ความสำคัญลำดับแรก**
- ระบบบริการประชาชน
- ระบบสำคัญ/เสี่ยงสูง
- ระบบที่จัดเก็บ/ประมวลผลข้อมูลส่วนบุคคลและข้อมูลสำคัญ
- บัญชีผู้ใช้งานที่มีสิทธิระดับสูง

**เพิ่มชั้นการป้องกัน**
เหนือกว่าการใช้ชื่อผู้ใช้งาน
และรหัสผ่านเพียงอย่างเดียว

**ยืนยันตัวตนเพิ่มเติม**
เช่น รหัสแบบใช้ครั้งเดียว (OTP)
หรือกลไกอื่นที่หน่วยงานกำหนด

**ลดโอกาสการเข้าถึงสำเร็จ**
แม้ Credential ถูกขโมย
หรือรั่วไหล

**ลดความเสี่ยงการยึดบัญชี**
และการเข้าถึงระบบ
โดยไม่ได้รับอนุญาต

**มาตรการเร่งด่วน**
- Reset Password ระบบที่สำคัญ ภายใน 2 วัน
- ปิดระบบที่ไม่ใช้งานทันที

**ขับเคลื่อนตามกรอบระยะเวลา**

| 15 วัน | 30 วัน | 60 วัน | 90 วัน | 180 วัน |
|---|---|---|---|---|
| เร่งดำเนินการในระบบสำคัญเร่งด่วน | ขยายผลการใช้ MFA และมาตรการที่เกี่ยวข้อง | ติดตามความก้าวหน้าและแก้ไขอุปสรรค | ประเมินผลและยกระดับการป้องกัน | สรุปผลและทบทวนมาตรการอย่างต่อเนื่อง |

ให้แต่ละกระทรวงแต่งตั้ง DPO เป็น Focal Point ระดับกระทรวง
ทำหน้าที่ศูนย์กลางประสานงาน กำกับ ติดตาม และรายงานผลอย่างเป็นระบบ

**มาตรการทดแทน**
สำหรับหน่วยงานที่ยังไม่สามารถเปิดใช้ MFA กับระบบสำคัญได้ทันที
- มีมาตรการทดแทนเพื่อลดความเสี่ยง
- จัดทำแผนแก้ไข ระบุผู้รับผิดชอบ
- กำหนดวันแล้วเสร็จชัดเจน

หัวหน้าหน่วยงานกำกับติดตามการดำเนินงานอย่างใกล้ชิด

**เตรียมประเทศไทยสู่ยุค Post-Quantum**
สั่งการให้ สกมช. ร่วมกับ สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ ดำเนินการเตรียมความพร้อมรองรับภัยคุกคามจากคอมพิวเตอร์ควอนตัม

สำรวจและจัดทำ Cryptographic Inventory → ประเมินความเสี่ยงด้านคริปโตกราฟี → จัดทำ PQC Migration Plan → เสนอคณะกรรมการดิจิทัลฯ และคณะรัฐมนตรีพิจารณาต่อไป

**ยกระดับความมั่นคงปลอดภัยไซเบอร์ของภาครัฐ**
คุ้มครองข้อมูลสำคัญของประเทศ | เสริมความเชื่อมั่น | ให้ประชาชนใช้บริการภาครัฐได้อย่างปลอดภัยและต่อเนื่อง

NCSA สกมช | ThaiCERT Thailand Computer Emergency Response Team
By NCSA Thailand

DETECT
ANALYZE
RESPOND
TOGETHER
FOR A SAFER THAILAND

# KEY TAKEAWAYS
## MFA | API | ACCESS CONTROL
## ยกระดับความปลอดภัย เริ่มได้จากพื้นฐานที่ถูกต้อง

STRONGER SECURITY  SAFER PEOPLE  A MORE RESILIENT THAILAND

"ความมั่นคงปลอดภัยไซเบอร์ คือ รากฐานของบริการที่ประชาชนไว้วางใจ"


"เทคโนโลยีที่มั่นคง เริ่มจาก "การใช้งานที่ปลอดภัย"

## 01 MFA
### Multi-Factor Authentication

ยืนยันตัวตนหลายปัจจัย
ลดความเสี่ยงจาก Credential รั่วไหล


- Something you know (Password)
- Something you have (OTP / Token)
- Something you are (Biometric)

**มติ ครม. 11 สิงหาคม 2569**
เห็นชอบให้หน่วยงานของรัฐยกระดับการยืนยันตัวตนแบบหลายปัจจัย (MFA) เช่น Digital Identity (ThaiD) หรือวิธีการยืนยันตัวตนรูปแบบอื่นที่มีความมั่นคงปลอดภัย โดยมอบหมายให้ สกมช. ขับเคลื่อนและติดตามการดำเนินการ

1. เร่งเปิดใช้ MFA สำหรับบัญชีผู้ดูและระบบ บัญชีสิทธิระดับสูง และบัญชีเข้าถึงจากภายนอก/ระยะไกล
2. ระบบที่ให้บริการประชาชน เชื่อมต่ออินเทอร์เน็ต หรือจัดเก็บ/ประมวลผลข้อมูลส่วนบุคคล ควรเร่งใช้ MFA
3. ลดความเสี่ยงจากการใช้ Username และ Password ที่อาจรั่วไหล แม้มีรหัสผ่านก็ไม่สามารถเข้าสู่ระบบได้ง่าย
4. สำหรับบริการที่สำคัญ ต้องกำหนดให้ใช้การยืนยันตัวตนหลายปัจจัยในการตรวจสอบสิทธิและเข้าใช้งาน
5. หากยังไม่สามารถใช้ MFA ได้ทันที ต้องมีมาตรการควบคุมทดแทน เช่น จำกัดแหล่งที่มา ทบทวนสิทธิ ตรวจจับพฤติกรรมผิดปกติ และระงับบัญชีที่ไม่ได้ใช้งาน

## 02 API
### Secure API Access

เชื่อมต่ออย่างปลอดภัย
ปกป้องข้อมูลตลอดการใช้งาน


1. ยืนยันตัวตนของทั้งผู้ใช้และระบบที่เรียกใช้ API ด้วยกลไกมาตรฐานที่มีความมั่นคงปลอดภัย
2. อนุญาตให้เข้าถึงเฉพาะ API Endpoint และทรัพยากรตามสิทธิที่กำหนด
3. จำกัดการเปิดเผยข้อมูลผ่าน API ให้สอดคล้องกับสิทธิของผู้เรียกใช้
4. กำหนดการควบคุมการใช้งาน เช่น Rate Limiting, Timeout, ขนาดข้อมูล และจำนวนคำขอพร้อมกัน
5. กำหนดรหัสหรือข้อความแสดงข้อผิดพลาด ไม่ให้เปิดเผยข้อมูลสำคัญ
6. จัดทำข้อตกลงเงื่อนไขความรับผิดชอบของผู้ใช้งาน API

## 03 ACCESS CONTROL

ควบคุมสิทธิการเข้าถึง ใช้งานเท่าที่จำเป็น


1. ใช้หลัก Least Privilege ให้สิทธิเท่าที่จำเป็น
2. แยกหน้าที่สำคัญ (Separation of Duties) เพื่อลดความเสี่ยง
3. จำกัดการเข้าถึงเฉพาะบุคลากร กิจกรรม อุปกรณ์ และ Interface ที่ได้รับอนุญาต
4. บริหารสิทธิ์โดยต่านี้ MFA ในการตรวจสอบสิทธิ และยืนยันตัวตน
5. ไม่ควรมี Shared Account ยกเว้นกรณีจำเป็นจริง
6. ติดตามกิจกรรมและพฤติกรรมผิดปกติของแต่ละบัญชี พร้อมแจ้งเตือน
7. ลบหรือปิดบัญชีที่ไม่ได้เข้งนหรือไม่จำใช้งน
8. ทบทวนสิทธิการใช้งานอย่างน้อยทุก 12 เดือน

ประชาชนมั่นใจ | บริการภาครัฐเดินหน้าต่อเนื่อง | ลดความเสี่ยงจากภัยไซเบอร์ | สร้างสังคมดิจิทัลที่ยั่งยืน

TOGETHER, WE ARE ThaiCERT