REPORT

รายงานสถิติ Cyber Attack เดือนเมษายน ปี 2025

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.)
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

Email: thaicert@ncsa.or.th
Website:
https://www.ncsa.or.th
https://www.thaicert.or.th

120 หมู่ 3 อาคารัฐประศาสนภักดี (อาคารบี) ชั้น 7 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา
5 ธันวาคม 2560 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210

คำนำ

รายงานผลการวิเคราะห์ Cyber Attack เดือนเมษายน ปี 2025 นี้จัดทำขึ้นเพื่อให้ข้อมูลเชิงลึกเกี่ยวกับสถิติเหตุการณ์โจมตีทางไซเบอร์ที่เกิดขึ้น โดยการวิเคราะห์เน้นแสดงประเภทของหน่วยงานที่ได้รับผลกระทบ ซึ่งประกอบด้วยหน่วยงานควบคุมหรือกำกับดูแล (Regulators) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) และหน่วยงานรัฐบาล (GOV) รวมถึงจำนวนเหตุการณ์ (Event) ที่เกิดขึ้นในเดือนดังกล่าว นอกจากนี้ รายงานยังได้นำเสนอแนวทางการป้องกันและรับมือที่สามารถนำไปใช้ได้จริง เพื่อเสริมสร้างความปลอดภัยในระบบไซเบอร์ ทั้งในระดับองค์กรและบุคคลทั่วไป พร้อมทั้งช่วยเตรียมความพร้อมในการลดความเสี่ยงจากภัยคุกคามที่ซับซ้อนและพัฒนารูปแบบอย่างต่อเนื่อง

รายงานฉบับนี้มีเป้าหมายเพื่อช่วยให้ผู้อ่านเข้าใจภาพรวมของสถานการณ์ Cyber Attack ได้ชัดเจนมากขึ้น และสามารถนำข้อมูลที่ได้ไปปรับใช้เพื่อยกระดับระบบป้องกันและสร้างความมั่นคงทางไซเบอร์ได้อย่างมีประสิทธิภาพในอนาคต

สารบัญ

ภาพรวม Cyber Attack เดือนเมษายน ปี 2025 ของหน่วยงานควบคุมหรือกำกับดูแล (Regulators) 1

ภาพรวม Cyber Attack เดือนเมษายน ปี 2025 ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ(CII) 2

ภาพรวม Cyber Attack เดือนเมษายน ปี 2025 ของหน่วยงานรัฐบาล (GOV) 3

แนวทางการป้องกันและรับมือ 4

ภาพรวม Cyber Attack เดือนเมษายน ปี 2025 ของหน่วยงานควบคุมหรือกำกับดูแล (Regulators)

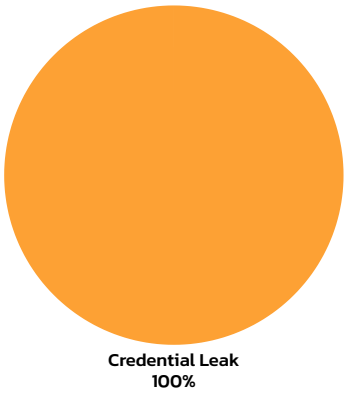
ในเดือนเมษายนที่ผ่านมา ไม่มีการตรวจพบเหตุการณ์ Cyber Attack ในหน่วยงานควบคุมหรือกำกับดูแล (Regulators) ซึ่งผลลัพธ์ดังกล่าวสะท้อนให้เห็นถึงการดำเนินมาตรการเชิงรุกด้านความปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพ อย่างไรก็ตาม ในยุคที่ภัยคุกคามทางไซเบอร์มีการพัฒนาอย่างรวดเร็วและมีความซับซ้อนมากขึ้น การเฝ้าระวังและการปรับปรุงมาตรการป้องกันอย่างต่อเนื่องยังคงมีความสำคัญ เพื่อให้สามารถรับมือจากภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในอนาคตได้อย่างทันท่วงทีและมีประสิทธิภาพสูงสุด

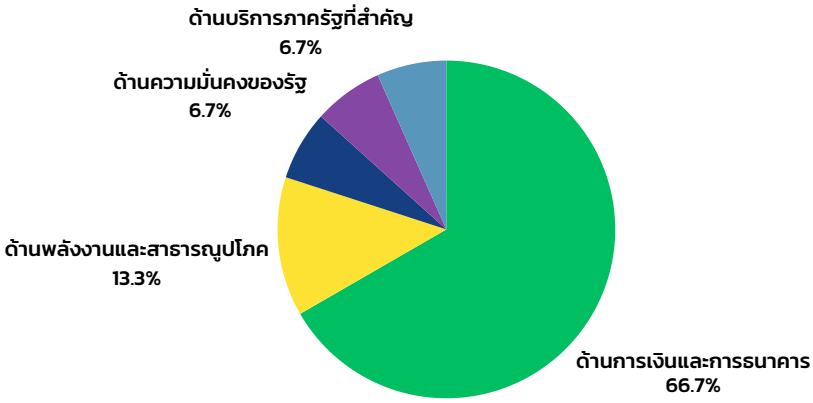
ภาพรวม Cyber Attack เดือนเมษายน ปี 2025 ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)

ในเดือนเมษายน ปี 2025 ที่ผ่านมา สถานการณ์ Cyber Attack ในหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ตรวจพบเหตุการณ์ Credential Leak รวม 15 เหตุการณ์ โดยแบ่งเป็นด้านการเงินและการธนาคาร 10 เหตุการณ์ รองลงมาด้านพลังงานและสาธารณูปโภค 2 เหตุการณ์ ด้านความมั่นคงของรัฐ 1 เหตุการณ์ ด้านบริการภาครัฐที่สำคัญ 1 เหตุการณ์ ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม 1 เหตุการณ์ ส่วนด้านการขนส่งและโลจิสติกส์และด้านสาธารณสุข ไม่พบ Credential Leak

ประเภทการโจมตี	Event(s)
Credential Leak	15

ประเภทหน่วยงาน	Event(s)
ด้านการเงินและการธนาคาร	10
ด้านพลังงานและสาธารณูปโภค	2
ด้านความมั่นคงของรัฐ	1
ด้านบริการภาครัฐที่สำคัญ	1
ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม	1
ด้านการขนส่งและโลจิสติกส์	0
ด้านสาธารณสุข	0



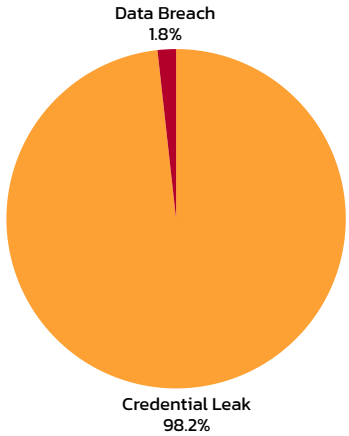


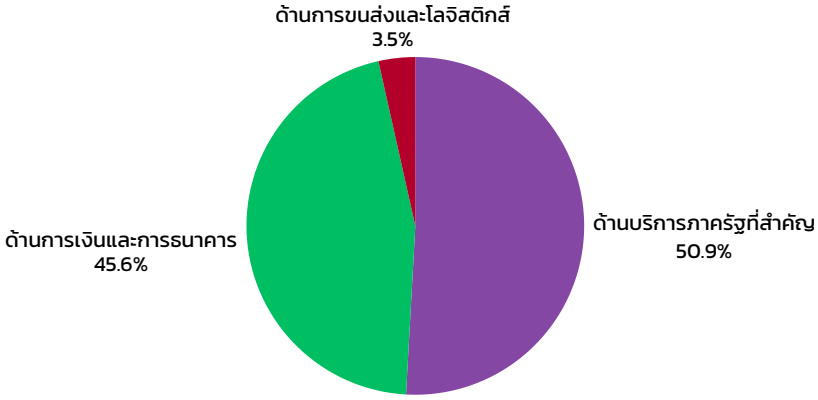
ภาพรวม Cyber Attack เดือนเมษายน ปี 2025 ของหน่วยงานรัฐบาล (GOV)

ในเดือนเมษายน ปี 2025 ที่ผ่านมา สถานการณ์ Cyber Attack ในหน่วยงานรัฐบาล (GOV) ตรวจพบเหตุการณ์ Credential Leak รวม 56 เหตุการณ์ โดยแบ่งเป็นด้านบริการภาครัฐที่สำคัญ 29 เหตุการณ์ ด้านการเงินและการธนาคาร 26 เหตุการณ์ ด้านการขนส่งและโลจิสติกส์ 1 เหตุการณ์ และพบ Data Breach 1 เหตุการณ์ คือ ด้านการขนส่งและโลจิสติกส์

ประเภทการโจมตี	Event(s)
Credential Leak	56
Data Breach	1

ประเภทหน่วยงาน	Event(s)
ด้านบริการภาครัฐที่สำคัญ	29
ด้านการเงินและการธนาคาร	26
ด้านการขนส่งและโลจิสติกส์	2
ด้านพลังงานและสาธารณูปโภค	0
ด้านความมั่นคงของรัฐ	0
ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม	0
ด้านสาธารณสุข	0





แนวทางการป้องกันและรับมือ

1. การป้องกันล่วงหน้า (Preventive Measures)

1.1 เสริมสร้างโครงสร้างพื้นฐานด้านความปลอดภัย

- Firewall & Intrusion Detection Systems (IDS/IPS): ติดตั้งไฟร์วอลล์และระบบตรวจจับการบุกรุก เพื่อตรวจจับและป้องกันการโจมตีในเครือข่าย
- Web Application Firewall (WAF): เพื่อป้องกันการโจมตีเว็บ เช่น SQL Injection และ Cross-Site Scripting (XSS)

1.2 ใช้การเข้ารหัส (Encryption)

- เข้ารหัสข้อมูลสำคัญทั้งที่จัดเก็บ (Data at Rest) และขณะถ่ายโอน (Data in Transit) ด้วย SSL/TLS เพื่อป้องกันการดักฟังและขโมยข้อมูล

1.3 การอัปเดตและแพตช์ระบบ

- อัปเดตระบบปฏิบัติการ, ซอฟต์แวร์, และปลั๊กอินอย่างสม่ำเสมอเพื่อปิดช่องโหว่ที่อาจถูกใช้โจมตี

1.4 การจัดการสิทธิ์ (Access Control)

- ใช้หลักการ Least Privilege (ให้สิทธิ์เท่าที่จำเป็น) และการยืนยันตัวตนแบบสองขั้นตอน (2FA)

2. การตรวจสอบและตรวจจับ (Monitoring and Detection)

2.1 ระบบตรวจสอบความผิดปกติ (SIEM)

- ใช้ระบบจัดการเหตุการณ์และข้อมูลด้านความปลอดภัย (Security Information and Event Management - SIEM) เพื่อวิเคราะห์และตรวจจับเหตุการณ์ที่ผิดปกติ

2.2 การตรวจสอบ Log

- ตรวจสอบ Log ของเซิร์ฟเวอร์และอุปกรณ์เครือข่ายเพื่อหากิจกรรมที่ผิดปกติ เช่น การเข้าถึงจาก IP แปลก ๆ หรือการพยายามล็อกอินที่ผิดพลาด

3. การตอบสนองเมื่อถูกโจมตี (Incident Response)

3.1 สร้างแผนตอบสนองเหตุการณ์ (Incident Response Plan)

- กำหนดทีมรับมือ (Incident Response Team) และแผนการปฏิบัติที่ชัดเจนเมื่อเกิดการโจมตี เช่น การกักกันภัยคุกคามและการกู้คืนระบบ

3.2 แยกระบบที่ถูกโจมตี

- หากตรวจพบการโจมตี ให้ตัดการเชื่อมต่ออุปกรณ์หรือเครือข่ายที่ได้รับผลกระทบออกจากระบบหลัก เพื่อลดการแพร่กระจาย

3.3 แจ้งเตือนและประสานงาน

- แจ้งผู้มีส่วนเกี่ยวข้อง เช่น ผู้บริหาร, ทีม IT, หรือเจ้าหน้าที่บังคับใช้กฎหมาย รวมถึงแจ้งผู้ใช้ในกรณีข้อมูลส่วนตัวถูกละเมิด

แนวทางการป้องกันและรับมือ

4. การฟื้นฟูและป้องกันในอนาคต (Recovery and Reinforcement)

4.1 สำรองข้อมูล (Data Backup)

- จัดเก็บข้อมูลสำรองในรูปแบบเข้ารหัส และทดสอบการกู้คืนข้อมูลเป็นระยะ

4.2 การประเมินเหตุการณ์ (Post-Incident Review)

- วิเคราะห์เหตุการณ์เพื่อตรวจสอบช่องโหว่และปรับปรุงกระบวนการป้องกันในอนาคต

4.3 การฝึกอบรมความปลอดภัย (Security Training)

- สร้างความตระหนักรู้ให้พนักงานเกี่ยวกับภัยคุกคามทางไซเบอร์ เช่น Phishing และ Social Engineering

References

- Threat Intelligence ฝ่ายบริหารจัดการข้อมูลภัยคุกคามทางไซเบอร์
- Recorded Future (TI)

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.)

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

Email: thaicert@ncsa.or.th
Website:
https://www.ncsa.or.th
https://www.thaicert.or.th

120 หมู่ 3 อาคารัฐประศาสนภักดี (อาคารบี) ชั้น 7 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา
5 ธันวาคม 2560 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210