REPORT

Indicator of Compromise เดือนมกราคม ปี 2025

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ
Thailand Computer Emergency Response Team (ThaiCERT)

120 หมู่ 3 อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น 7 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
โทรศัพท์ 02 142 6888 (ติดต่อเวลาทำการ)
โทรสาร 02 143 7593
Email: thaicert[at]ncsa.or.th
แจ้งเหตุภัยคุกคามไซเบอร์: thaicert[at]ncsa.or.th

คำนำ

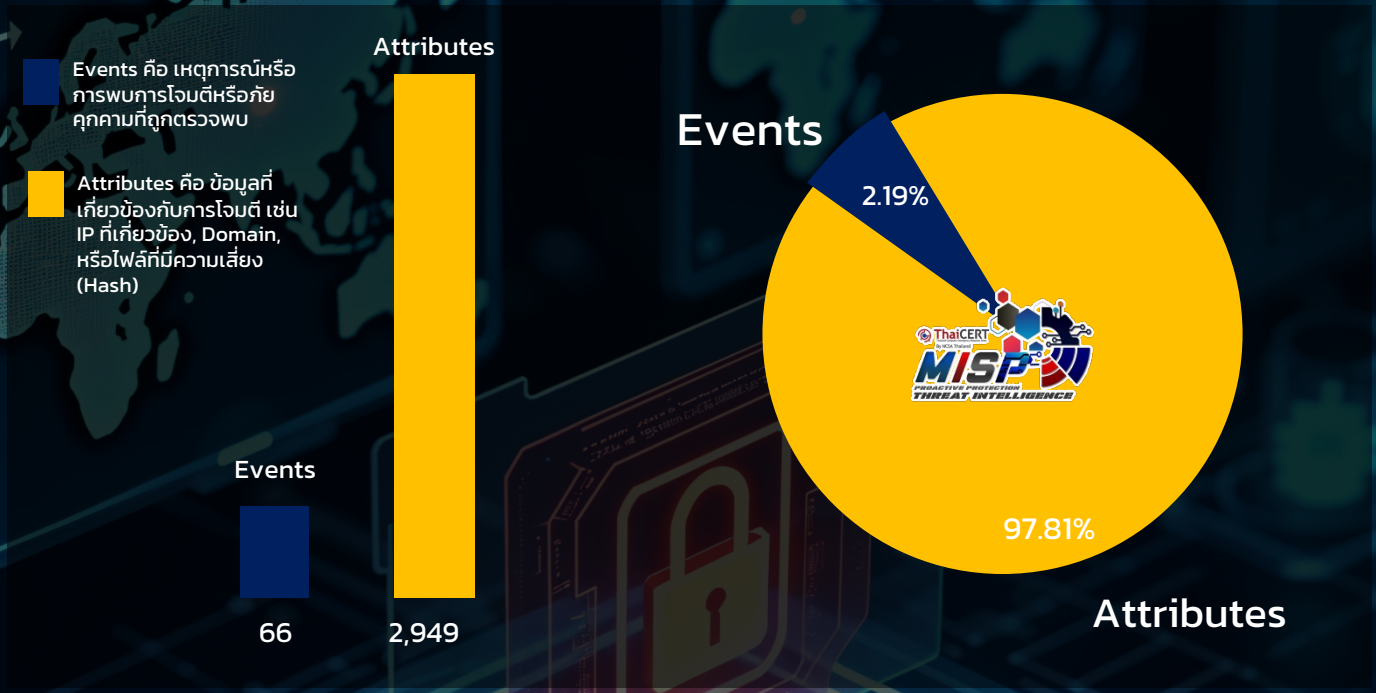
จากการรวบรวมและวิเคราะห์ข้อมูล Indicator of Compromise (IoCs) ในเดือนมกราคม ปี 2025 พบว่ามีการโจมตีที่เพิ่มขึ้นอย่างมีนัยสำคัญในหลายภาคส่วนฝ่ายบริหารจัดการข้อมูลภัยคุกคามทางไซเบอร์ได้จัดทำรายงานสรุปผลการวิเคราะห์นี้ขึ้นเพื่อให้เห็นภาพรวมของข้อมูลสถานการณ์การโจมตีในเดือนมกราคม ปี 2025

รายงานนี้มีวัตถุประสงค์เพื่อให้ข้อมูลที่เป็นประโยชน์แก่ผู้ที่เกี่ยวข้องในการป้องกันและรับมือกับการโจมตีจากภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพโดยเน้นถึงความสำคัญของการเตรียมความพร้อมและการตอบสนองต่อภัยคุกคามที่เกิดขึ้นอย่างรวดเร็วและมีประสิทธิภาพ

ทั้งนี้ หวังเป็นอย่างยิ่งว่ารายงานนี้จะเป็นประโยชน์ในการเสริมสร้างความรู้และความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ที่กำลังเพิ่มขึ้นในปัจจุบัน รวมถึงวิธีการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์สำหรับทุกภาคส่วนได้อย่างมีประสิทธิภาพและปลอดภัย

ภาพรวม การวิเคราะห์ Indicator of Compromise (IoCs) ในเดือนมกราคม ปี 2025

ในเดือนมกราคม ปี 2025 พบว่าสถิติการรวบรวมและวิเคราะห์ข้อมูล Indicator of Compromise (IoCs) จากการโจมตีของภัยคุกคามทางไซเบอร์ มีจำนวนเพิ่มขึ้นอย่างต่อเนื่อง ดังนั้น ฝ่ายบริหารจัดการข้อมูลภัยคุกคามทางไซเบอร์ จึงได้จัดประเภทหมวดหมู่ของ Indicator of Compromise (IoCs) ที่ได้วิเคราะห์ลงในระบบ MISP (Malware Information Sharing Platform and Threat Sharing) สำหรับการรับและแบ่งปันเหตุการณ์ภัยคุกคามทางไซเบอร์ เป็นดังนี้



จากภาพ แสดงให้เห็นว่า ในแต่ละ Events ที่ได้วิเคราะห์นั้น จะมี จำนวน Attributes ที่หลากหลายและแตกต่างกันไป ซึ่งในเดือนมกราคม ปี 2025 ได้รวบรวมและวิเคราะห์ข้อมูล Indicator of Compromise (IoCs) จำนวน 66 Events และ 2,949 Attributes จากการนำข้อมูลทั้ง 66 Events มาเปรียบเทียบกับข้อมูลทั้งหมด จะพบว่า Events คิดเป็นเพียง 2.19% ในขณะที่ข้อมูล Attributes ซึ่งเป็นข้อมูลที่เกี่ยวข้องกับแต่ละเหตุการณ์ จะคิดเป็น 99.81% ของข้อมูลทั้งหมด

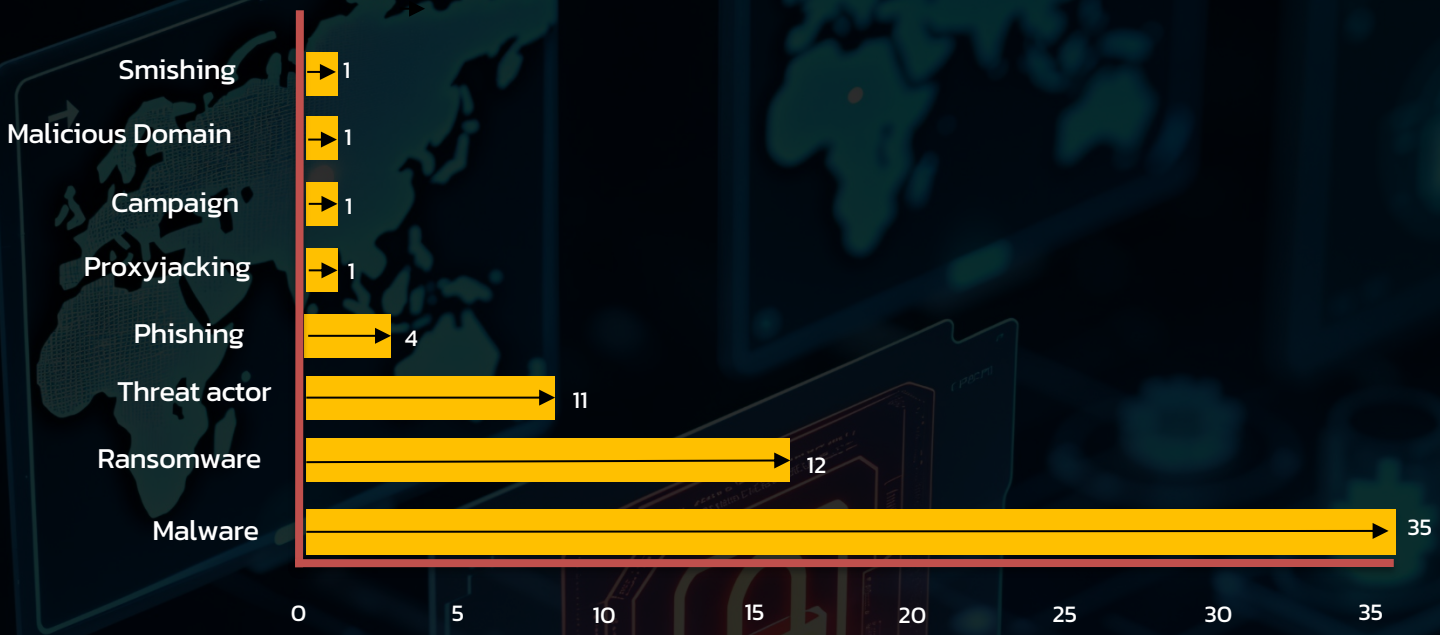
สาเหตุที่ Attributes มีจำนวนมากกว่า Events อย่างมาก

หนึ่ง Event สามารถมีหลาย Attributes : ในแต่ละเหตุการณ์ (Event) ที่ตรวจพบ อาจมีหลาย (IoCs) เช่น
- มัลแวร์ตัวเดียว อาจมีหลาย Hash (MD5, SHA-1, SHA-256)
- โดเมนที่ใช้โจมตี อาจมีหลาย IP ที่เกี่ยวข้อง
- Phishing Campaign อาจมีหลาย URL ที่ใช้ล่อลวง

โครงสร้างของ IoCs มีรายละเอียดเยอะ : IoCs ไม่ใช่แค่การบอกว่า "มีการโจมตีเกิดขึ้น" แต่ต้องมีรายละเอียด เช่น
- IP Address ของผู้โจมตี
- URL ที่ถูกใช้ในการโจมตี
- มัลแวร์ที่เกี่ยวข้อง

ประเภทของภัยคุกคามทางไซเบอร์ ที่ได้จากการวิเคราะห์ Indicator of Compromise (IoCs) ในเดือนมกราคม ปี 2025

แบ่งออกเป็น 8 ประเภทดังนี้



จัดลำดับ ดังนี้

- ลำดับที่ 1 Malware 35 จำนวน
- ลำดับที่ 2 Ransomware 12 จำนวน
- ลำดับที่ 3 Threat actor 11 จำนวน
- ลำดับที่ 4 Phishing 4 จำนวน

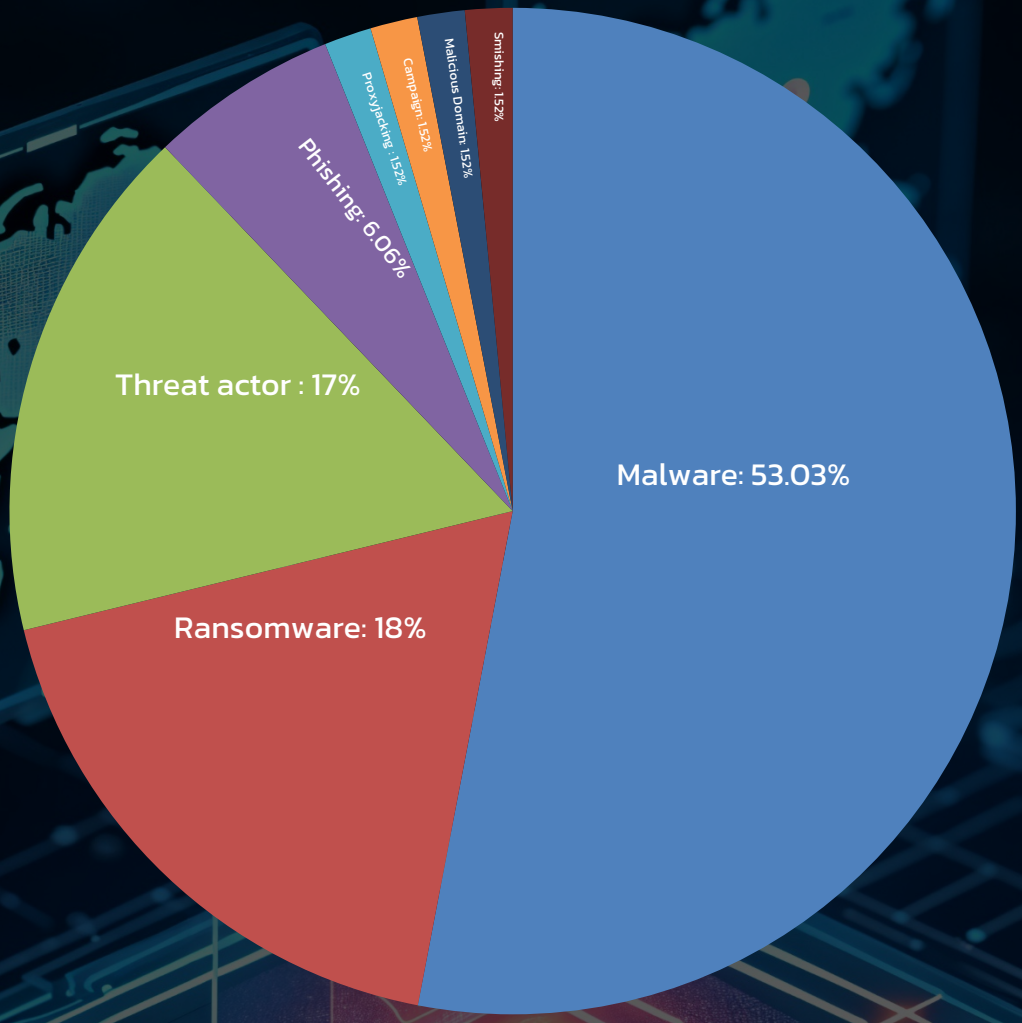
อื่น ๆ

- Proxyjacking 1 จำนวน
- Campaign 1 จำนวน
- Malicious Domain 1 จำนวน
- Smishing 1 จำนวน

Malware เป็นประเภทที่พบมากที่สุด (มากกว่าครึ่งหนึ่งของทั้งหมด)
Ransomware และ Threat actor ก็นับเป็นกลุ่มที่มีสัดส่วนสูง
ประเภททั่วไป เช่น Proxyjacking, Smishing, และ Campaign มีจำนวนค่อนข้างน้อย

ประเภทของภัยคุกคามทางไซเบอร์ ที่ได้จากการวิเคราะห์ Indicator of Compromise (IoCs) ในเดือนมกราคม ปี 2025

สรุปเป็นภาพรวม ดังนี้



จากภาพ สรุปได้ว่า จำนวน Malware ที่ได้ถูกรวบรวมและวิเคราะห์ข้อมูล Indicator of Compromise (IoCs) ในเดือนมกราคม ปี 2025 นั้น มีจำนวนที่สูงที่สุด เป็นเปอร์เซ็นที่ 53.03% ต่อด้วยจำนวน Ransomware เป็นเปอร์เซ็นที่ 18% ตามมาด้วยจำนวน Threat actor เป็นเปอร์เซ็นที่ 17%, Phishing เป็นเปอร์เซ็นที่ 6.06%, Proxyjacking 1.52%, Campaign 1.52%, Malicious Domain 1.52% และ Smishing 1.52%

แนวทางการป้องกันและรับมือกับภัยคุกคามไซเบอร์

การป้องกันและรับมือกับภัยคุกคามไซเบอร์ที่มีความหลากหลาย เช่น Malware, Ransomware, Threat Actors, Tool-based Attacks, Vulnerabilities, Phishing, Campaign Attacks, และ Data Leaks จำเป็นต้องมีแนวทางที่ครอบคลุมและสอดคล้องกับประเภทของภัยคุกคามนั้น ๆ ด้านล่างนี้ คือแนวทางที่สามารถนำไปปรับใช้ได้

1. Malware
   - ป้องกัน:
     - ใช้ซอฟต์แวร์ป้องกันไวรัสที่อัปเดตล่าสุดในทุกอุปกรณ์
     - ปรับปรุงระบบปฏิบัติการและซอฟต์แวร์ให้ทันสมัยเสมอ
     - ใช้ระบบไฟร์วอลล์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
   - รับมือ:
     - แยกอุปกรณ์ที่ติดมัลแวร์ออกจากเครือข่ายทันที
     - สแกนอุปกรณ์ทั้งหมดเพื่อหาการติดเชื้อเพิ่มเติม
     - สำรองข้อมูลอย่างสม่ำเสมอเพื่อกู้คืนข้อมูลในกรณีที่จำเป็น
2. Ransomware
   - ป้องกัน:
     - ใช้ระบบสำรองข้อมูลอัตโนมัติและเก็บข้อมูลสำรองไว้นอกเครือข่าย
     - บังคับใช้นโยบายการรักษาความปลอดภัย เช่น การจำกัดสิทธิ์ของผู้ใช้งาน
     - ฝึกอบรมพนักงานให้ระมัดระวังไฟล์แนบในอีเมลและลิงก์ที่ไม่ชัดเจน
   - รับมือ:
     - อย่าชำระค่าไถ่เด็ดขาด (ยกเว้นกรณีมีคำสั่งเฉพาะ)
     - แจ้งเหตุการณ์ให้กับเจ้าหน้าที่ไซเบอร์หรือ CERT ของประเทศ
     - ฟื้นฟูระบบจากข้อมูลสำรอง
3. Threat Actors
   - ป้องกัน:
     - ใช้การพิสูจน์ตัวตนแบบหลายชั้น (Multi-Factor Authentication)
     - ตรวจสอบกิจกรรมในระบบเครือข่ายเพื่อตรวจจับพฤติกรรมที่ผิดปกติ
     - ติดตั้งระบบ SIEM (Security Information and Event Management) เพื่อแจ้งเตือนภัยคุกคาม
   - รับมือ:
     - บันทึกข้อมูลที่เกี่ยวข้องกับการโจมตีเพื่อนำไปวิเคราะห์
     - ใช้ระบบ EDR (Endpoint Detection and Response) เพื่อจัดการกับภัยคุกคามในจุดเชื่อมต่อ

แนวทางการป้องกันและรับมือกับภัยคุกคามไซเบอร์

4. Tool-based Attacks
   - ป้องกัน:
     - ตรวจสอบและบันทึกการใช้งานเครื่องมือหรือซอฟต์แวร์ที่อาจถูกนำไปใช้โจมตี
     - จำกัดการเข้าถึงเครื่องมือที่อาจเป็นอันตรายให้เฉพาะผู้ที่ได้รับอนุญาต
   - รับมือ:
     - ยกเลิกสิทธิ์การใช้งานเครื่องมือที่ถูกใช้ในทางที่ไม่เหมาะสม
     - อัปเดตระบบตรวจจับภัยคุกคาม (IDS/IPS) เพื่อรองรับรูปแบบใหม่
5. Vulnerabilities
   - ป้องกัน:
     - ทำการทดสอบเจาะระบบ (Penetration Testing) เป็นประจำ
     - แก้ไขช่องโหว่ในซอฟต์แวร์ทันทีที่มีแพตช์อัปเดต
   - รับมือ:
     - ปิดการเข้าถึงส่วนที่มีช่องโหว่จนกว่าจะมีการแก้ไข
     - แจ้งเตือนผู้ใช้ในเครือข่ายเกี่ยวกับช่องโหว่ที่ตรวจพบ
6. Phishing
   - ป้องกัน:
     - ใช้โซลูชันอีเมลที่สามารถกรองสแปมและฟิชชิงได้
     - สร้างความตระหนักรู้ให้ผู้ใช้ในการตรวจจับอีเมลฟิชชิง
   - รับมือ:
     - ยกเลิกการเข้าถึงบัญชีที่ตกเป็นเหยื่อ
     - ตรวจสอบกิจกรรมที่น่าสงสัยที่เกิดขึ้นหลังการโจมตี
7. Campaign Attacks
   - ป้องกัน:
     - ตรวจสอบการเข้าถึงและกิจกรรมที่ผิดปกติในโครงสร้างพื้นฐาน IT
     - ใช้ Threat Intelligence เพื่อระบุและป้องกันแคมเปญที่เป็นอันตราย
   - รับมือ:
     - ประสานงานกับผู้เชี่ยวชาญด้านความปลอดภัยเพื่อวิเคราะห์และตอบโต้การโจมตี
     - แจ้งองค์กรอื่น ๆ ในวงการเกี่ยวกับการโจมตีเพื่อป้องกันการแพร่กระจาย
8. Data Leaks
   - ป้องกัน:
     - เข้ารหัสข้อมูลสำคัญทั้งในระหว่างการส่งและการเก็บรักษา
     - ใช้ DLP (Data Loss Prevention) เพื่อป้องกันการรั่วไหลของข้อมูล
   - รับมือ:
     - แจ้งลูกค้าหรือผู้ที่ได้รับผลกระทบทันที
     - วิเคราะห์แหล่งที่มาของการรั่วไหลและอุดช่องโหว่ที่เกิดขึ้น

References

- Threat Intelligence ฝ่ายบริหารจัดการข้อมูลภัยคุกคามทางไซเบอร์

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ
Thailand Computer Emergency Response Team (ThaiCERT)

120 หมู่ 3 อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น 7 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
โทรศัพท์ 02 142 6888 (ติดต่อเวลาทำการ)
โทรสาร 02 143 7593
Email: thaicert[at]ncsa.or.th
แจ้งเหตุภัยคุกคามไซเบอร์: thaicert[at]ncsa.or.th