ทำความรู้จักกับ

THREAT ACTOR

ผู้ร้ายในโลกดิจิทัล

นายปิยพนธ์ ปั้นนาค
เจ้าหน้าที่บริหารงานทั่วไป

ภัยคุกคามโลกดิจิทัลในปัจจุบันมีรูปแบบการโจมตีที่หลากหลาย ซึ่งล้วนแต่เป้าหมายเพื่อสร้างความเสียหายแก่องค์กร หรืออาจสร้างความเสียหายร้ายแรงถึงระดับประเทศ การที่จะเกิดภัยไซเบอร์ได้ ต้องอาศัยผู้ก่ออาชญากรรม ที่เรียกว่า **Threat Actor (หรือ แฮกเกอร์)** โดยการนำวิธีการและมัลแวร์ต่าง ๆ เข้ามาโจมตี เหยื่อ (NT cyfence. 2567)

Threat Actor คือใคร

"Threat Actor" หรือ "ผู้คุกคามทางไซเบอร์" หมายถึงบุคคลหรือกลุ่มที่มีจุดมุ่งหมายในการโจมตีระบบคอมพิวเตอร์ เครือข่าย หรือข้อมูลขององค์กร เพื่อประโยชน์ตนเอง โดยมีเป้าหมายในการแทรกแซงความเป็นส่วนตัว การโจรกรรมข้อมูลสำคัญขององค์กร นอกจากนี้อาจสร้างความเสียหายด้านชื่อเสียง ไปจนถึงการใช้ Ransomware ล็อคข้อมูลสำคัญ และอาจทำให้เกิดการหยุดชะงักในการดำเนินธุรกิจได้

Threat Actor เป็นบุคคล หรือกลุ่มคน

Threat Actor อาจหมายถึงบุคคลหรือกลุ่มคนที่มีส่วนเกี่ยวข้องในกิจกรรมที่เป็นภัยคุกคามต่อระบบคอมพิวเตอร์ หรือข้อมูลที่สามารถเป็นได้ทั้งบุคคลคนเดียวหรือเป็นกลุ่มประกอบด้วย

- **บุคคลเดียว (Individual)** เช่น แฮกเกอร์ (Hacker) ที่ทำการโจมตีเพื่อตนเองหรือเป้าหมายอื่น ๆ
- **กลุ่ม (Group)** เช่น กลุ่มอาชญากรรมทางไซเบอร์ (Cybercriminal Group) ที่มีการจัดตั้งเพื่อโจมตีระบบต่าง ๆ ตามเป้าหมาย
- **องค์กรหรือรัฐ (Organization or State)** เช่น หน่วยงานที่มีการสนับสนุนจากรัฐบาลเพื่อทำกิจกรรมด้านภัยคุกคามทางไซเบอร์

“Threat Actor”

ตัวอย่างของกลุ่ม Threat Actor

- **RansomHub** กลุ่มนี้เป็น Ransomware-as-a-Service (RaaS) เน้นการเรียกค่าไถ่และเป้าหมายเน้นกลุ่มเป้าหมายที่มีชื่อเสียง
- **Qilin Ransomware** กลุ่มนี้ได้รับความสนใจจากการโจมตี Synnovis ในสหราชอาณาจักร
- **Dark Angels (Dunghill Leak)** กลุ่มนี้เป็นที่รู้จักจากการเปิดเผยข้อมูลขององค์กรใหญ่และรัฐบาล โดยมีการเรียกค่าไถ่ที่สูงถึง 75 ล้านดอลลาร์สหรัฐ
- **APT29 (The Dukes)** กลุ่มนี้มักจะมาจากประเทศรัสเซีย มีการโจมตีทางอิเล็กทรอนิกส์ที่เน้นการเข้าระบบและการเก็บข้อมูลทางการเงิน
- **TA542 (Emotet)** กลุ่มนี้เป็น cybercriminal ที่มีการโจมตีทางอินเทอร์เน็ตที่เน้นการแพร่กระจายไวรัสและการเก็บข้อมูลทางการเงิน
- **LockBit** เป็นกลุ่ม ransomware ที่มีชื่อเสียงมาก และเป็นที่รู้จักในฐานะ Ransomware-as-a-Service (RaaS) ที่มีการใช้งานอย่างกว้างขวาง

ประเภทของ Threat Actor 6 กลุ่มหลัก

- **ผู้โจมตีที่มีจุดประสงค์ทางการเมือง (Hacktivists)** กลุ่มนี้มักจะมีเป้าหมายที่เกี่ยวข้องกับการแสดงออกทางการเมืองหรือสังคม โดยจะโจมตีเพื่อเผยแพร่ประเด็นทางการเมืองหรือสังคม
- **อาชญากรไซเบอร์ (Cybercriminals)** กลุ่มที่โจมตีเพื่อผลประโยชน์ทางการเงิน เช่น การโจมตี ransomware และ phishing เพื่อขโมยข้อมูล เป็นกลุ่มที่มุ่งหวังผลประโยชน์ทางการเงินจากการโจมตีโดยเฉพาะ
- **รัฐบาลที่สนับสนุนสงครามไซเบอร์ (Nation-state actors)** รัฐบาลมักสนับสนุนผู้กระทำการที่เป็นภัยโดยมีเป้าหมายในการขโมยข้อมูลที่เป็นความลับ รวบรวมข้อมูลที่สำคัญ หรือทำให้โครงสร้างพื้นฐานที่สำคัญของรัฐบาลอื่นหยุดชะงัก รวมถึงการสอดแนม (espionage) หรือสงครามไซเบอร์ (cyberwarfare) มีการสนับสนุนทางการเงินสูง ทำให้ภัยคุกคามเหล่านี้มีความซับซ้อนและยากที่จะตรวจจับ
- **ผู้ที่โจมตีเพื่อความสนุก (Thrill seekers)** กลุ่มคนที่โจมตีระบบคอมพิวเตอร์และข้อมูลเพื่อความสนุกสนาน อยากใช้การแฮกเพื่อเข้าใจวิธีการทำงานของเครือข่ายและระบบคอมพิวเตอร์มากขึ้น หนึ่งในกลุ่มนี้คือ “script kiddies” จะไม่มีทักษะทางเทคนิคสูง แต่ใช้เครื่องมือและเทคนิคที่มีอยู่แล้วเพื่อโจมตีระบบที่อ่อนแอ โดย ทำเพื่อความบันเทิงหรือความพอใจส่วนตัว อาจทำให้เกิดความเสียหายโดยไม่ตั้งใจ เช่น การรบกวนความเสถียรของเครือข่าย ซึ่งอาจเป็นช่องทางให้มีการโจมตีใหม่ในอนาคตได้

ประเภทของ Threat Actor 6 กลุ่มหลัก (ต่อ)

- **กลุ่มที่มีเป้าหมายทำให้เกิดความรุนแรงทางไซเบอร์เพื่อเหตุผลทางการเมือง** (Cyberterrorists) กลุ่มคนที่โจมตีทางไซเบอร์โดยมีแรงจูงใจหรืออุดมการณ์ทางการเมือง มีเป้าหมายคือการสร้างความกลัวหรือก่อให้เกิดความรุนแรง บางคนในกลุ่มนี้อาจได้รับการสนับสนุนจากรัฐ

- **คนที่ก่อความเสียหายทั้งโดยเจตนาหรือจากความผิดพลาด** (Insider threats) คนที่ก่อความเสียหายจากความผิดพลาด (Human Error) เช่น การติดตั้งมัลแวร์โดยไม่รู้ตัว ซึ่งอาชญากรทางไซเบอร์สามารถนำช่องโหว่ตรงนี้ไปใช้ในการเข้าถึงเครือข่ายได้ รวมไปถึงกลุ่มคนที่มีเจตนาร้าย เช่น พนักงานที่ไม่พอใจและใช้สิทธิ์การเข้าถึงข้อมูลเพื่อขโมยข้อมูลไปใช้เพื่อผลประโยชน์ส่วนตัว เช่น ผลประโยชน์ทางการเงิน หรือทำลายข้อมูลภายในระบบ

การป้องกันการโจมตีจากบรรดาเหล่า Threat Actor

หลักการป้องกันการโจมตีจากบรรดาเหล่า Threat Actor เป็นสิ่งสำคัญที่องค์กรต่าง ๆ ควรให้ความสนใจโดยการใช้เทคโนโลยีและแนวทางที่เหมาะสมในการป้องกัน ดังนี้

- **การฝึกอบรมพนักงาน** เพื่อให้รู้จักการตรวจจับและหลีกเลี่ยงการโจมตี และช่วยในการป้องกันภัยคุกคาม พนักงานจึงควรได้รับการฝึกอบรมอย่างสม่ำเสมอ โดยการสอนวิธีสังเกตอีเมล Phishing และแนะนำการปฏิบัติที่ปลอดภัยในการใช้งานอินเทอร์เน็ต
- **การใช้ระบบป้องกันและตรวจจับภัยคุกคาม องค์กรควรติดตั้งระบบ Firewall และระบบตรวจจับการโจมตีแบบ IDS/IPS** (Intrusion Detection and Prevention Systems) เพื่อช่วยกรองข้อมูลที่เข้าสู่ระบบ ตรวจจับพฤติกรรมที่ผิดปกติ และป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต
- **การสำรองข้อมูล (Backup)** การสำรองข้อมูลเป็นสิ่งสำคัญเพื่อให้มั่นใจได้ว่าสามารถกู้คืนข้อมูลได้ในกรณีที่ถูกโจมตี จึงควรสำรองข้อมูลอย่างสม่ำเสมอและเก็บข้อมูลสำรองได้ในที่ที่ปลอดภัย เช่น ในระบบคลาวด์หรือฮาร์ดดิสก์ที่แยกออกจากเครือข่ายหลัก
- **การอัปเดตซอฟต์แวร์และระบบปฏิบัติการ** สามารถช่วยปิดช่องโหว่ที่อาจถูก Threat Actor ใช้เจาะระบบได้ โดยองค์กรควรมีนโยบายการอัปเดตซอฟต์แวร์ทุกครั้งที่มีเวอร์ชันใหม่เพื่อให้มั่นใจว่าระบบมีความปลอดภัยที่สุด
- **การตรวจสอบและทดสอบระบบรักษาความปลอดภัยอย่างสม่ำเสมอ** การตรวจสอบและทดสอบระบบ (เช่น การทดสอบการเจาะระบบ หรือ Penetration Testing) ช่วยค้นหาช่องโหว่ที่อาจจะเกิดขึ้น และเป็นการยืนยันว่ามาตรการที่ใช้อยู่มีประสิทธิภาพในการป้องกันภัยคุกคาม

รายการอ้างอิง

NT cyfence. (2567, 13 พฤศจิกายน). **ทำความรู้จักกับ Threat Actor ผู้ร้ายในโลกดิจิทัล.** https://www.cyfence.com/article/what-is-threat-actor/