สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

การกระทำ - ผลกระทบ

Physical Security

- บุกรุก
- วางเพลิง
- ลักทรัพย์

- ทำให้เกิดความหวาดกลัว
- ทรัพย์สินเสียหาย
- ทรัพย์สินเสียหาย

Cyber Security

บุกรุก
- Hacking

ก่อกวน
- DDOS

Malware
- Computer Virus
- Trojan Horse
- Worms
- Ransomware

Social Engineering
- Web Phishing
- Vishing
- Spear Phishing

Virus การโจมตีด้วยการพรางตัวเองไปกับไฟล์ต่าง ๆ แพร่กระจายโดยอาศัยไฟล์พาหะ ไฟล์ในเครื่องที่ถูกโจมตีจะเกิดความเสียหายอย่างหนัก

Worm การโจมตีด้วยการพรางตัวเองไปกับไฟล์ต่าง ๆ แพร่กระจายโดยอาศัยไฟล์พาหะ ไฟล์ในเครื่องที่ถูกโจมตีจะเกิดความเสียหายอย่างหนัก

Trojan Horse เป็นมัลแวร์ที่ปลอมตัวเป็นไฟล์ธรรมดา จะทำการเปิดประตูให้ระบบเพื่อโจมตีขั้นถัดไป เพื่อล้วงข้อมูล แอบดูกิจกรรมการใช้งานคอมพิวเตอร์ รหัสผ่าน

Rootkit เป็นมัลแวร์ที่มีคุณสมบัติการเข้าถึงสิทธิพิเศษของระบบและพรางตัวไม่ให้ถูกจับได้ ติดตั้งตนเองโดยอาศัยช่องโหว่ของระบบ เมื่อเสร็จแล้วยากต่อการตวจจับและลบทิ้ง

Ransomware ล็อคไฟล์ในเครื่องไม่ให้เข้าถึงได้ บังคับให้ผู้ใช้จ่ายเงินเพื่อแลกกับรหัสปลดล็อคไฟล์

Keylogger เน้นการดักจับข้อมูลการใช้งานคีบอร์ด เพื่อขโมยรหัสผ่านไปใช้ผลประโยชน์

Garyware เป็นมัลแวร์ที่สร้างความน่ารำคาญให้กับผู้ใช้ แต่อย่างเลวร้าวที่สุด ทำหน้าที่แอบดูได้เหมือน Keylogger ด้วย

Malware

Cryptojacking ฝังตัวตามหน้าเว็ปไซด์ ทำงานด้วย JavaScript เป้าหมายคือการใช้คอมพิวเตอร์ของเราขุดเหมืองดิจิทัล

Malvertising การใช้โฆณาบนโลกออนไลน์ เพื่อแพร่กระจายมัลแวร์

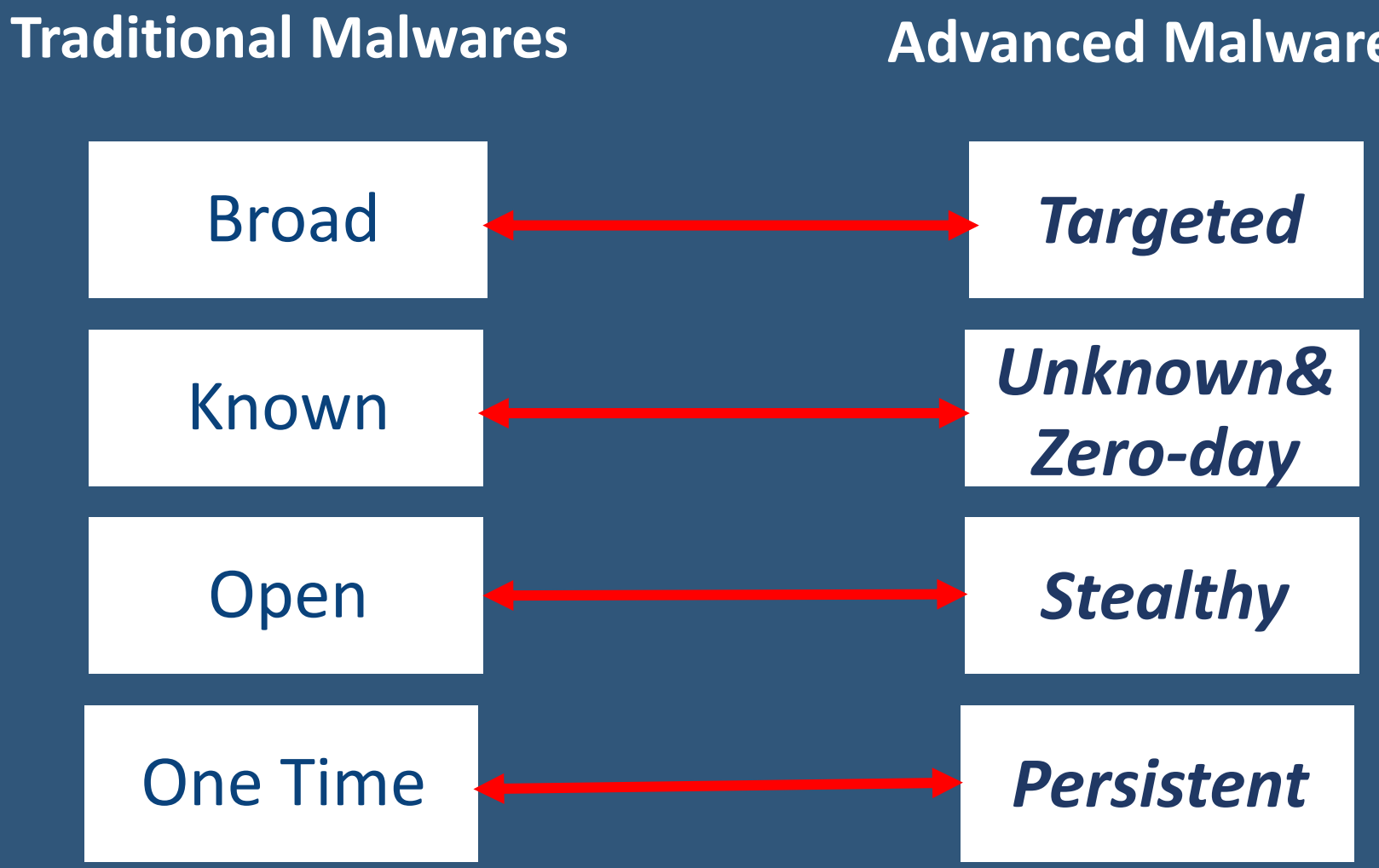
Crimeware เป็นเครื่องมือแฮกสำหรับผู้ที่ไม่มีทักษะในการแฮก ใช้เพื่อส่องจอหรือเก็บข้อมูลการใช้คีย์บอร์ด

Bots Botnets ทำให้เป้าหมายล่ม ส่งสแปม แพร่กระจายมัลแวร์ เพื่อทำให้เครื่องเหยื่อเป็น Bots ไปด้วย

Fileless Maware ใช้เครื่องมือของระบบปฏิบัติการในการเริ่มขั้นตอการโจมตี ทำงานบนแรมทำให้หายไปอย่างไร้ร่องรอยเมื่อปิดเครื่อง

Spyware เป็นมัลแวร์ที่มีเป้าหมายในการเก็บรวบรวมข้อมูลของผู้ใช้ เพื่อส่งกลับไปยังแฮกเกอร์เพื่อส่งข้อมูลไปขายต่อ

Adware เป็นโฆษณาที่ติดมาพร้อมกับตัวติดตั้งซอฟแวร์ทั่วไป ไม่ได้สร้างอันตรายต่อผู้ใช้แต่สร้างความน่ารำคาญมากกว่า


Traditional Malwares
Advanced Malwares
Broad
Targeted
Known
Unknown&
Zero-day
Open
Stealthy
One Time
Persistent

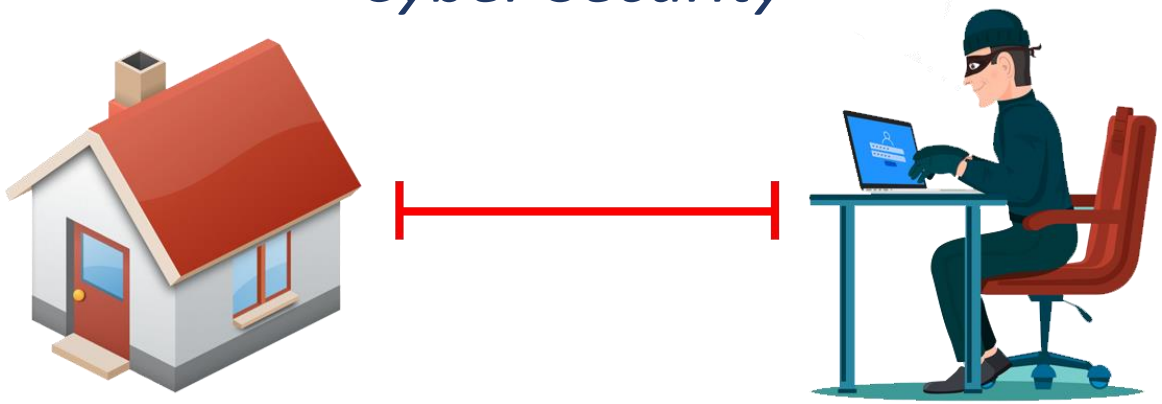
ความแตกต่างสำคัญ

Physical Security

- กล้องวงจรปิด ลายนิ้วมือ คราบเลือด DNA
- การเชื่อมโยงหลักฐานกับข้อเท็จจริง

ความเสียหายที่มองเห็นในวงจำกัด

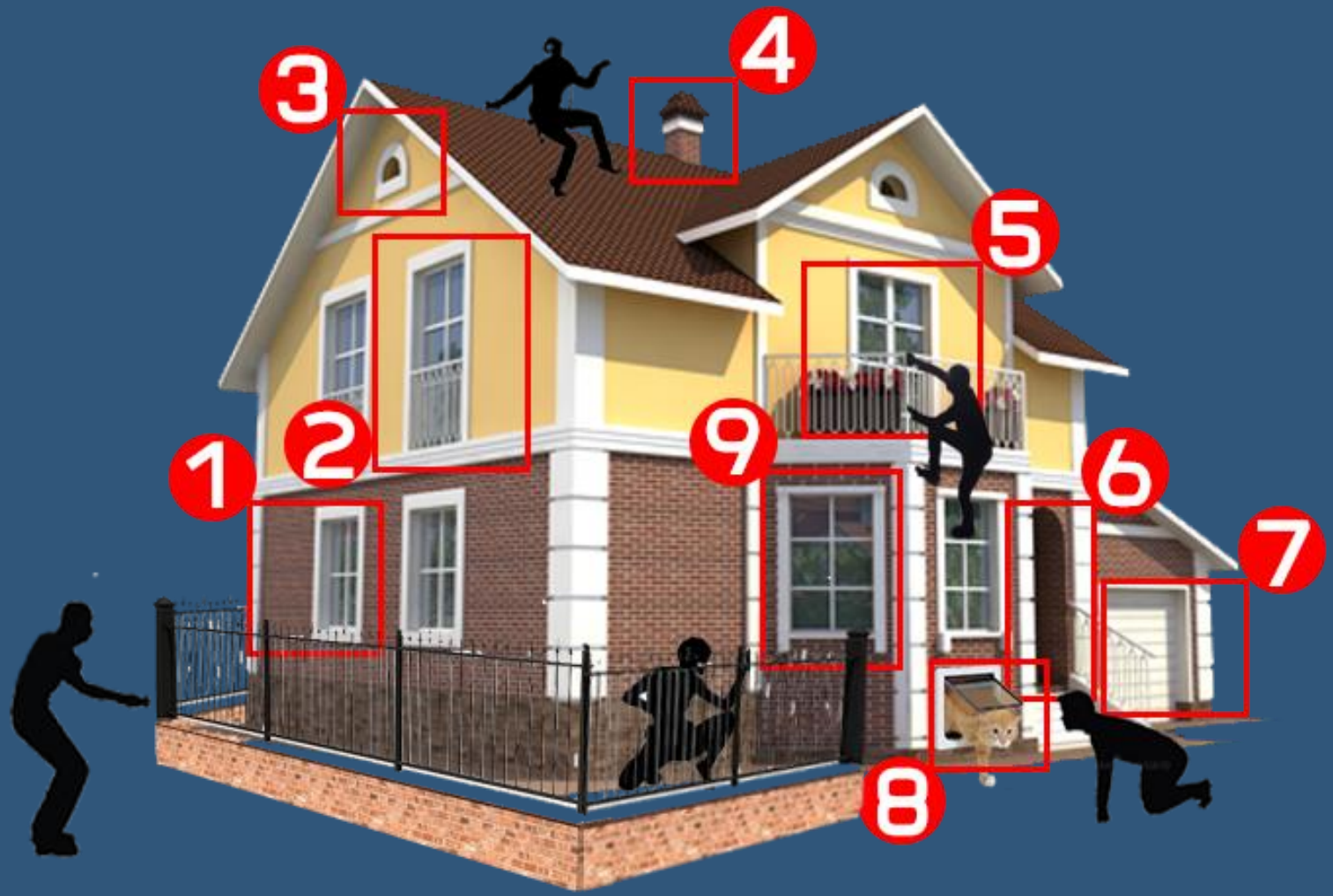
Cyber Security

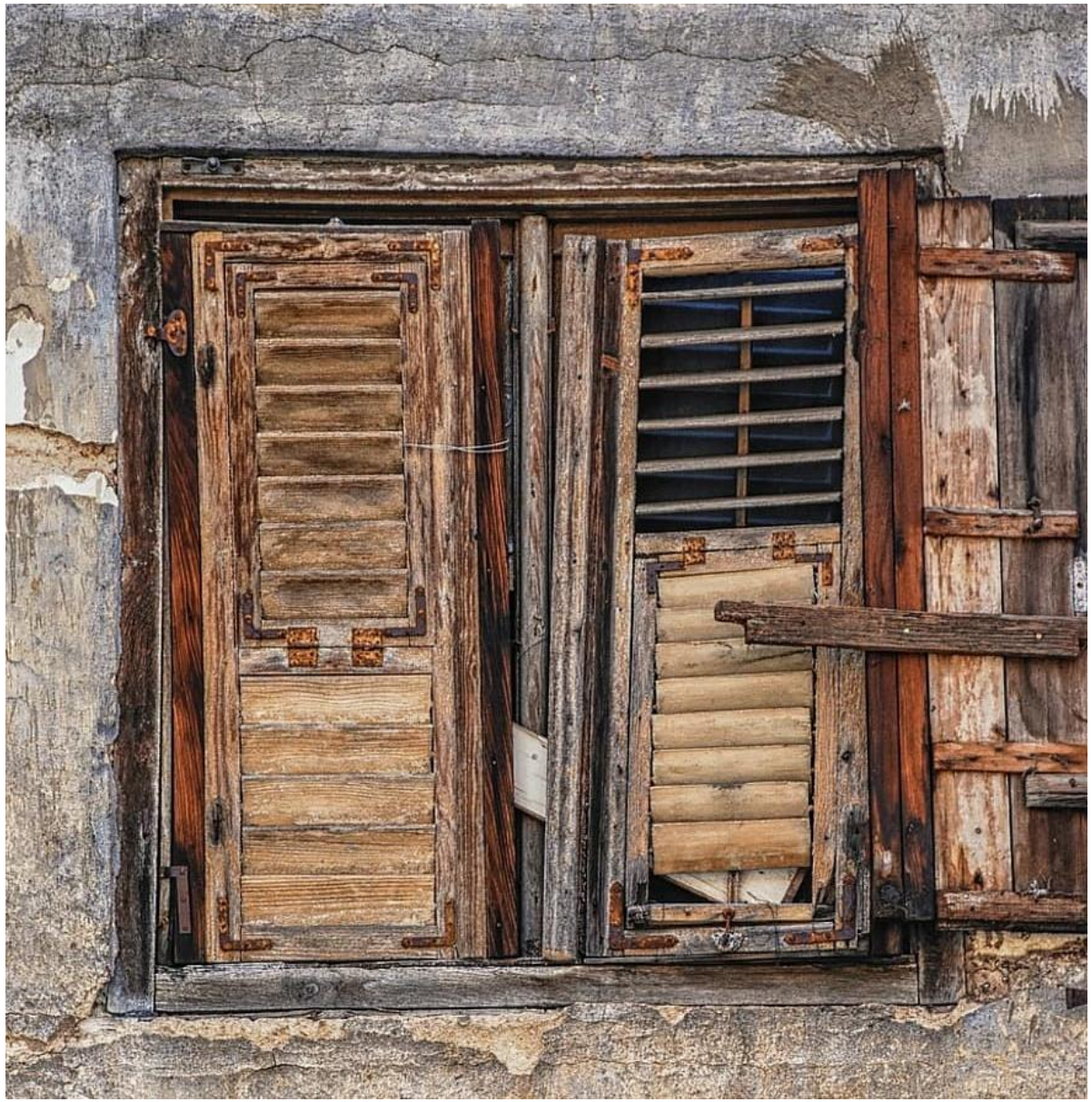


- Network traffic forensic
- Computer forensic analysis
- Malware analysis

ความเสียหายเกิดเป็นวงกว้าง
ข้อมูลรั่วไหลเป็นสาธารณะ

ทุกระบบมี ช่องโหว่





ภัยคุกคามไซเบอร์

- ดูจะเป็นเรื่องการตั้งรับ
- Security is journey
- มีโอกาสเกิดขึ้นในวันใดวันหนึ่ง
- จับก็ยาก ไล่ก็ไม่ทัน
- หาวิธีที่ดีที่สุดเพื่อลดความเสี่ยง

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)