แจ้งเตือน : เฝ้าระวัง

Alert

**ผลกระทบทางธุรกิจ**

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

**ผลกระทบต่อระบบ**

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

# แจ้งเตือนเพื่อเฝ้าระวัง Supply Chain Attack ผ่านซอฟต์แวร์ DAEMON Tools

**วันที่แจ้งเตือน 14 พฤษภาคม 2569**

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้เผยแพร่รายงานความเสี่ยงด้านภัยคุกคามไซเบอร์กรณีทีมวิจัยจาก Kaspersky ตรวจพบ Supply Chain Attack ผ่านซอฟต์แวร์ DAEMON Tools (โปรแกรม Virtual Drive และจัดการ Disk Image) โดยพบว่าไฟล์ติดตั้งจากเว็บไซต์ทางการของผู้พัฒนาได้ถูกฝังโค้ดอันตราย (ตั้งแต่วันที่ 8 เมษายน 2569) เมื่อผู้ใช้งานติดตั้งโปรแกรมดังกล่าวแล้วจะถูกติดตั้ง Backdoor ลงในระบบ เพื่อส่งข้อมูลของเครื่องเหยื่อไปยังผู้ไม่หวังดี ทั้งนี้ พบเป้าหมายอยู่ในหน่วยงานภาครัฐ หน่วยงานวิทยาศาสตร์ ภาคการผลิต และค้าปลีก ในประเทศเบลารุส รัสเซีย รวมถึง**ประเทศไทย**

ThaiCERT ได้ออกคำแนะนำในการเฝ้าระวัง และ แนวทางการดำเนินการดังนี้

| | |
|---|---|
| **ผลิตภัณฑ์และระบบที่ได้รับผลกระทบ** | 1. DAEMON Tools Lite เวอร์ชันฟรี ที่ดาวน์โหลดหรือติดตั้ง ตั้งแต่วันที่ 8 เมษายน 2569<br>2. DAEMON Tools เวอร์ชัน 12.5.0.2421 ถึง 12.5.0.2434 ซึ่งมีรายงานว่าถูกฝังโค้ดอันตราย<br>3. ระบบปฏิบัติการ Windows ที่มีการติดตั้งไฟล์ติดตั้งที่ได้รับผลกระทบ<br>4. หน่วยงานที่อนุญาตให้ผู้ใช้งานติดตั้งซอฟต์แวร์จากอินเทอร์เน็ตโดยไม่มีการตรวจสอบความปลอดภัยเพิ่มเติม |
| **แนวทางการตรวจสอบและป้องกัน** | 1. ตรวจสอบว่ามีการใช้งาน DAEMON Tools Lite เวอร์ชันฟรี โดยเฉพาะเครื่องที่ติดตั้งหรืออัปเดตโปรแกรมตั้งแต่วันที่ 8 เมษายน 2569<br>2. ถอนการติดตั้ง DAEMON Tools Lite เวอร์ชันที่ได้รับผลกระทบ และ**ติดตั้งเวอร์ชันล่าสุดที่ผู้พัฒนาเผยแพร่แล้วเท่านั้น**<br>3. ทำการสแกนระบบด้วยโปรแกรม Antivirus, EDR หรือระบบตรวจจับภัยคุกคาม เพื่อค้นหา Backdoor หรือ มัลแวร์ที่อาจถูกติดตั้ง<br>4. ตรวจสอบพฤติกรรมการเชื่อมต่อเครือข่ายที่ผิดปกติ เช่น การเชื่อมต่อออกไปยังปลายทางที่ไม่รู้จักหรือการสื่อสารผ่านโปรโตคอล QUIC (Quick UDP Internet Connections) ที่ผิดปกติ |
| **แนวทางลดความเสี่ยงชั่วคราว** | 1. พิจารณาแยกเครื่องที่มีการติดตั้ง DAEMON Tools ออกจากเครือข่ายของหน่วยงานชั่วคราว<br>2. เปลี่ยนรหัสผ่านบัญชีสำคัญที่เคยใช้งานบนเครื่องที่อาจได้รับผลกระทบ โดยเฉพาะบัญชี Domain Admin, VPN และระบบภายในหน่วยงาน<br>3. ตรวจสอบ Log การเข้าถึงระบบย้อนหลังตั้งแต่วันที่ 8 เมษายน 2569 เพื่อค้นหาพฤติกรรมที่ผิดปกติหรือการเข้าถึงที่ไม่ได้รับอนุญาต<br>4. สำรองข้อมูลสำคัญอย่างสม่ำเสมอ และทดสอบกระบวนการกู้คืนระบบเพื่อรองรับกรณีเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย |

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

**ข้อมูลอ้างอิง**


1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 12 พ.ค. 2569
2. https://www.securityweek.com/government-scientific-entities-hit-via-daemon-tools-supply-chain-attack/
3. https://www.bleepingcomputer.com/news/security/daemon-tools-devs-confirm-breach-release-malware-free-version/?