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 มัลแวร์ Trojan JscealTaskExec โจมตีระบบปฏิบัติการ Windows

วันที่แจ้งเตือน 29 เมษายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้เผยแพร่รายงานความเสี่ยงด้านภัยคุกคามไซเบอร์ กรณี Microsoft ตรวจพบ Trojan: Win32/JScealTaskExec โดยอุปกรณ์ที่ถูกติดตั้งมัลแวร์ดังกล่าวอาจตรวจพบอาการ เช่น ประสิทธิภาพการทำงานช้าลง, มีการเปลี่ยนแปลงการตั้งค่าหน้าจอเดสก์ท็อป, เครื่องค้างหรือโปรแกรมหยุดการทำงาน (Crash) และพื้นที่จัดเก็บข้อมูลลดน้อยลง เป็นต้น

ThaiCERT ได้ออกคำแนะนำในการเฝ้าระวังและแนวทางการดำเนินการ ดังนี้

ปัจจัยเสี่ยงที่ควรระวัง:

- มัลแวร์สามารถเข้าสู่เครื่องได้หลายช่องทาง เช่น ไฟล์หรือโปรแกรมที่ดาวน์โหลดจากเว็บไซต์ภายนอก ไฟล์ที่แชร์ผ่านเครือข่าย peer-to-peer เว็บไซต์ที่ถูกแฮกหรือฝังโค้ดอันตราย และมัลแวร์ตัวอื่นที่ดาวน์โหลดภัยคุกคามเพิ่มเติมเข้ามาในเครื่อง เป็นต้น
- ผู้ใช้งานควรหลีกเลี่ยงการดาวน์โหลดซอฟต์แวร์จากแหล่งที่ไม่น่าเชื่อถือ เช่น โปรแกรม Crack, Keygen, โปรแกรมละเมิดลิขสิทธิ์ เว็บไซต์ดาวน์โหลดที่ไม่ทราบแหล่งที่มา หรือเว็บไซต์สตรีมมิ่งผิดกฎหมาย เป็นต้น เนื่องจากพฤติกรรมดังกล่าวอาจเพิ่มความเสี่ยงต่อการติดมัลแวร์หรือโปรแกรมไม่พึงประสงค์

แนวทางป้องกัน:

1. อัปเดต Microsoft Defender Antivirus และฐานข้อมูลตรวจจับให้เป็นปัจจุบันทันที และดำเนินการรัน Full scan เพื่อค้นหาและกำจัดร่องรอยที่อาจยังหลงเหลืออยู่ในระบบ
2. หากตรวจพบมัลแวร์ให้ใช้ Microsoft Defender Offline scan เพื่อตรวจจับมัลแวร์ที่ซ่อนตัวขณะที่ระบบกำลังทำงานได้ ทั้งนี้ ก่อนเริ่ม Offline scan ควรบันทึกงานทั้งหมดเนื่องจากเครื่องจะ restart ก่อนเริ่มการสแกน
3. ตรวจสอบผลการดำเนินการใน Protection history และหากพบรายการ Threat found – action needed ควรเลือก Quarantine (ไม่ควรเลือก Allow on device โดยไม่จำเป็น)
4. ตรวจสอบ Allowed threats เพื่อทบทวนรายการภัยคุกคามที่ผู้ใช้เคยอนุญาตไว้

ผู้ดูแลระบบ ควรตรวจสอบและจัดการความเสี่ยงที่เหมาะสม ดังนี้

1. มี Scheduled Task หรือ Startup entry ที่ไม่คุ้นเคยหรือไม่
2. มีไฟล์สคริปต์ เช่น js, .vbs, jse, ps1 หรือไฟล์ .exe อยู่ในโฟลเดอร์ชั่วคราวหรือโฟลเดอร์ผู้ใช้หรือไม่
3. มีโปรเซสผิดปกติที่ทำงานซ้ำหลังเปิดเครื่องหรือไม่
4. มีโปรแกรมที่เพิ่งติดตั้งจากแหล่งไม่น่าเชื่อถือหรือไม่
5. มีการเพิ่มข้อยกเว้นใน Antivirus โดยไม่ได้รับอนุญาตหรือไม่
6. มีการแจ้งเตือนซ้ำหลัง restart หรือหลังสแกนแล้วหรือไม่

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

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 29 เม.ย. 2569
2. https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan%3AWin32%2FJScealTaskExec.A