# เอกสารการแจ้งเตือนกรณีมัลแวร์ Yokai มุ่งเป้าโจมตีหน่วยงานในประเทศไทย เพื่อเข้าถึงข้อมูลสำคัญ

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เกี่ยวกับกรณีมัลแวร์ Yokai มุ่งเป้าโจมตีหน่วยงานในประเทศไทย เพื่อเข้าถึงข้อมูลสำคัญ ซึ่งการโจมตีทางไซเบอร์นี้ ใช้เทคนิคที่เรียกว่า DLL side-loading เพื่อส่งมัลแวร์ backdoor ที่ชื่อว่า Yokai ซึ่งมีความสามารถในการเข้าควบคุมระบบ และรับคำสั่งจากผู้โจมตีผ่านเซิร์ฟเวอร์ควบคุม Command and Control Server (C2 Server) โดยกระบวนการนี้เริ่มต้นจากไฟล์ RAR ที่แนบมากับอีเมล ซึ่งภายในมี Windows shortcut สองไฟล์ ชื่อภาษาไทยว่า "กระทรวงยุติธรรมสหรัฐ.pdf" (United States Department of Justice.pdf) และ "รัฐบาลสหรัฐขอความร่วมมือระหว่างประเทศในเรื่องทางอาญา.dock" (United States government requests international collaboration in criminal matters.dock) เมื่อเปิดไฟล์ ระบบจะเปิดเอกสาร PDF หรือ Word เพื่อเบี่ยงเบนความสนใจขณะเดียวกันมัลแวร์จะถูกติดตั้งในพื้นหลังอย่างลับ ๆ มัลแวร์นี้ออกแบบมาเพื่อปล่อยไฟล์เพิ่มเติมอีกสามไฟล์ ซึ่งรวมถึงไฟล์ที่ดูเหมือนถูกต้องจากโปรแกรมกู้คืนข้อมูล iTop Data Recovery ซึ่งไฟล์นี้จะถูกใช้เพื่อโหลด DLL อันตรายเข้าสู่ระบบ Yokai Backdoor จะตั้งค่าการทำงานซ้ำบนเครื่องเป้าหมาย พร้อมทั้งเชื่อมต่อไปยังเซิร์ฟเวอร์ควบคุม (C2 Server) เพื่อรับคำสั่ง เช่น การเปิดหน้าต่างคำสั่ง (cmd.exe) และรับคำสั่ง Shell เพื่อเข้าควบคุมระบบ [1]

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้งานใช้หลีกเลี่ยงการดาวน์โหลด และติดตั้งซอฟต์แวร์ที่ไม่ทราบแหล่งที่มา ตรวจสอบความถูกต้องของเว็บไซต์ก่อนทำการดาวน์โหลดแอปพลิเคชัน อัปเดตระบบปฏิบัติการ และซอฟต์แวร์ป้องกันไวรัสให้เป็นเวอร์ชันปัจจุบัน ระมัดระวังการเปิดไฟล์ที่ไม่ทราบแหล่งที่มา และหลีกเลี่ยงการรันสคริปต์ หรือโปรแกรมที่ไม่ได้รับการยืนยัน และสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

https://webboard-nsoc.ncsa.or.th/

**อ้างอิง**


1. https://thehackernews.com/2024/12/thai-officials-targeted-in-yokai.html
2. https://otx.alienvault.com/pulse/6760376bf27390cebc69add4