วันที่ 21 กรกฎาคม 2569

Daxin กลับมาเคลื่อนไหวอีกครั้งในไต้หวัน พร้อมพบ Stupig แบ็กดอร์ที่ทำงานในระดับ SYSTEM ได้ตั้งแต่ก่อนล็อกอิน

มัลแวร์ขั้นสูงที่ก่อนหน้านี้ถูกเชื่อมโยงกับกลุ่มผู้โจมตีทางไซเบอร์ที่มีความเกี่ยวข้องกับจีน ได้กลับมาปรากฏตัวอีกครั้งหลังหายไปนานกว่า 4 ปี โดยครั้งนี้ถูกตรวจพบภายในบริษัทผู้ผลิตแห่งหนึ่งในไต้หวัน พร้อมกับการค้นพบแบ็กดอร์ตัวใหม่ที่ไม่เคยมีการเปิดเผยมาก่อน ซึ่งมีชื่อว่า Stupig

Daxin (ไฟล์ "srt64.sys") ซึ่งเป็นรูทคิต (Rootkit) ที่ทำงานในระดับเคอร์เนลของระบบปฏิบัติการ Windows ถูกเปิดเผยครั้งแรกโดย Symantec ซึ่งปัจจุบันอยู่ภายใต้ Broadcom เมื่อเดือนมีนาคม 2022 โดยหลักฐานระบุว่า มัลแวร์ตัวนี้ถูกใช้ในการโจมตีแบบเจาะจงเป้าหมายต่อหน่วยงานรัฐบาลและโครงสร้างพื้นฐานสำคัญมาตั้งแต่ปี 2013 จากผลการวิเคราะห์ล่าสุดของทีม Symantec และ Carbon Black Threat Hunter Team พบว่า Daxin ยังคงถูกใช้งานอยู่ หลังตรวจพบว่าทำงานอยู่บนเครื่องที่ถูกเจาะระบบในไต้หวันเมื่อปี 2026 โดยเครื่องดังกล่าวเป็นของบริษัทลูกในไต้หวันที่อยู่ภายใต้ผู้ผลิตเทคโนโลยีข้ามชาติรายหนึ่ง และยังพบว่ามีการติดตั้ง Stupig (ไฟล์ "a.dll" หรือ "kbdus1.dll") อยู่บนเครื่องเดียวกันอีกด้วย

ชื่อไฟล์ "kbdus1.dll" ถูกตั้งขึ้นเพื่อให้ดูคล้ายกับ "kbdus.dll" ซึ่งเป็นไฟล์ DLL ของ Microsoft ที่ใช้สำหรับการจัดการคีย์บอร์ดภาษาอังกฤษ (สหรัฐฯ) เพื่อหลอกให้ดูเหมือนไฟล์ปกติของระบบ

Broadcom ระบุว่า Stupig ใช้เทคนิคที่ยังไม่เคยพบในมัลแวร์ตระกูลใดมาก่อน โดยใช้ไฟล์ DLL สำหรับคีย์บอร์ดที่ถูกดัดแปลงให้ทำงานผ่านกระบวนการ winlogon.exe ส่งผลให้ผู้โจมตีสามารถสั่งรันคำสั่งด้วยสิทธิ์ SYSTEM ได้โดยตรงตั้งแต่หน้าจอล็อกอิน ก่อนที่ผู้ใช้จะลงชื่อเข้าใช้ และไม่ทำให้เกิดเหตุการณ์บันทึกการล็อกอิน (Logon Audit Event) ใดๆ

สิ่งที่น่าสนใจคือ ทั้ง Daxin และ Stupig มีค่า Compilation Timestamp หรือเวลาที่ระบุว่าไฟล์ถูกคอมไพล์ อยู่ในช่วงต้นปี 2013 เหมือนกัน แม้ว่าเครื่องที่ติดมัลแวร์จะเพิ่งเริ่มส่งข้อมูล Telemetry ออกมาเมื่อวันที่ 12 พฤษภาคม 2026 ด้วยความสามารถของกลุ่มผู้โจมตีที่สามารถซ่อนตัวอยู่ในระบบได้เป็นเวลานาน นักวิจัยจึงคาดว่า การโจมตีครั้งนี้อาจดำเนินมาอย่างเงียบๆ และไม่ถูกตรวจพบเป็นเวลานานถึง 13 ปี

แม้ว่าจะยังไม่พบความเหมือนกันของโค้ดระหว่าง Daxin และ Stupig แต่การที่มัลแวร์ทั้งสองถูกติดตั้งอยู่บนเครื่องเดียวกัน มีหน้าที่ทำงานที่เสริมกัน ใช้แนวทางการพัฒนาที่คล้ายกัน และมีเวลาคอมไพล์ตรงกันในปี 2013 ทำให้นักวิจัยเชื่อว่า ทั้งสองอาจเป็นผลงานของผู้โจมตีกลุ่มเดียวกัน

Daxin มีวิธีการสื่อสารกับเซิร์ฟเวอร์ควบคุม (Command-and-Control หรือ C2) ที่แตกต่างจากมัลแวร์ทั่วไป โดยแทนที่จะสร้างการเชื่อมต่อออกไปยังเซิร์ฟเวอร์ของผู้โจมตีโดยตรง มัลแวร์ในระดับเคอร์เนลจะคอยตรวจสอบทราฟฟิก TCP ที่เข้ามา หากพบรูปแบบข้อมูลที่กำหนดไว้ ก็จะเข้าไปแทรกการเชื่อมต่อที่ถูกต้องตามปกติและใช้ช่องทางนั้นสำหรับรับส่งข้อมูลที่เข้ารหัสกับผู้โจมตี ทำให้การสื่อสารกลมกลืนไปกับทราฟฟิกปกติของระบบ นอกจากนี้ Daxin ยังสามารถสื่อสารกับเครื่องที่ไม่ได้เชื่อมต่ออินเทอร์เน็ตโดยตรงได้อีกด้วย

Broadcom อธิบายว่า วิธีการนี้ทำให้ Daxin ตรวจจับได้ยากมากด้วยการเฝ้าระวังทราฟฟิกเครือข่ายแบบทั่วไป อีกทั้งมัลแวร์ยังรองรับการสื่อสารแบบหลายทอด (Multi-hop) ผ่านเครื่องที่ติดมัลแวร์หลายเครื่อง ทำให้ผู้โจมตีสามารถเข้าถึงระบบที่ถูกแยกออกจากเครือข่ายภายนอกได้

ปัจจุบันยังไม่ทราบแน่ชัดว่าเครื่องดังกล่าวถูกเจาะระบบตั้งแต่เมื่อใดหรือด้วยวิธีใด แต่มีข้อสันนิษฐานว่า จุดเริ่มต้นอาจมาจากการใช้ระบบ Digiwin Single Sign-On (SSO) เวอร์ชันเก่า ซึ่งยังใช้งาน Java Development Kit (JDK) 1.5 และ 1.6 ที่หมดระยะการสนับสนุนไปแล้ว โดยติดตั้งมาตั้งแต่ช่วงปี 2009–2011

ทีมวิจัยอธิบายเพิ่มเติมว่า Stupig เป็นแบ็กดอร์ในรูปแบบ DLL ที่สร้างการทำงานแบบถาวร (Persistence) ด้วยการลงทะเบียนตัวเองเป็นผู้ให้บริการคีย์บอร์ด (Keyboard Layout Provider) ทำให้ win32k.sys โหลดไฟล์นี้เข้าไปใน winlogon.exe ทุกครั้งที่ระบบเริ่มทำงาน พร้อมกันนั้น DLL ดังกล่าวยังส่งคืนค่า KBDTABLES Pointer ที่ถูกต้อง ทำให้ฟังก์ชันของคีย์บอร์ดยังคงทำงานได้ตามปกติ จึงไม่สร้างความผิดสังเกตให้กับผู้ดูแลระบบหรือโปรแกรมที่ตรวจสอบโมดูลที่ถูกโหลดอยู่ในหน่วยความจำ

เมื่อ Stupig เริ่มทำงานภายใน winlogon.exe แล้ว มันจะคอยตรวจสอบชื่อผู้ใช้ที่ถูกพิมพ์บนหน้าจอล็อกอิน หากพบว่าชื่อผู้ใช้ขึ้นต้นด้วยคำว่า "stupig" ข้อความที่พิมพ์ต่อจากคำนี้จะถูกตีความเป็นคำสั่งและถูกรันทันทีด้วยสิทธิ์ SYSTEM

หากผู้โจมตีพิมพ์เพียงคำว่า "stupig" โดยไม่มีคำสั่งต่อท้าย มัลแวร์จะเปิดหน้าต่าง Command Prompt ที่ทำงานด้วยสิทธิ์ SYSTEM ขึ้นมาบนหน้าจอล็อกอินทันที การค้นพบ Daxin อีกครั้งในปี 2026 แสดงให้เห็นว่า ปฏิบัติการจารกรรมทางไซเบอร์นี้ไม่เคยยุติลงอย่างแท้จริง แต่เพียงลดการเคลื่อนไหวและคงการฝังตัวอยู่ในเครือข่ายของเป้าหมายอย่างเงียบๆ เพื่อหลีกเลี่ยงการตรวจจับ

Symantec และ Carbon Black กล่าวทิ้งท้ายว่า ด้วยการซ่อนตัวอยู่ภายในกระบวนการ Windows Logon และลงทะเบียนตัวเองเป็นผู้ให้บริการคีย์บอร์ด ทำให้ Stupig เปิดโอกาสให้ผู้โจมตีสามารถรันคำสั่งในระดับ SYSTEM และขโมยข้อมูลรับรองการเข้าสู่ระบบได้ตั้งแต่ก่อนที่ผู้ใช้จะล็อกอิน ซึ่งเป็นวิธีการที่ผู้ดูแลระบบส่วนใหญ่ยังไม่รู้จักและไม่ได้เฝ้าระวัง แม้ว่าจะยังไม่สามารถยืนยันได้ว่าผู้พัฒนามัลแวร์ทั้งสองตัวเป็นกลุ่มเดียวกันหรือไม่ แต่ความสามารถของทั้งคู่สามารถทำงานเสริมกันได้อย่างชัดเจน

การเปิดเผยครั้งนี้เกิดขึ้นพร้อมกับที่บริษัท Hunt.io รายงานว่า พบกลุ่มผู้โจมตีที่คาดว่ามีความเชื่อมโยงกับจีน ใช้โมเดลปัญญาประดิษฐ์ Anthropic Claude Code และ DeepSeek เพื่อช่วยทำให้การโจมตีทางไซเบอร์ต่อหน่วยงานภาครัฐและสถาบันการเงินใน อัฟกานิสถาน ไทย ไต้หวัน และสหรัฐอเมริกา เป็นแบบอัตโนมัติมากขึ้น การค้นพบดังกล่าวอ้างอิงจาก Open Directory ที่อยู่บนเซิร์ฟเวอร์ 112.213.124[.]132 ซึ่งมีลักษณะของ HTTP Header ตรงกับโครงสร้างพื้นฐานสำหรับควบคุมและสั่งการ (C2) ของ TencShell ที่เคยถูกระบุไว้ก่อนหน้านี้

Hunt.io ระบุว่า โมเดลเหล่านี้ถูกใช้ในการวิเคราะห์วิธีหลบเลี่ยงการป้องกัน ปรับแก้โค้ดโจมตีเมื่อการโจมตีล้มเหลว รวมถึงสร้างหน้าเว็บไซต์ฟิชชิงสำหรับหลอกขโมยข้อมูลบัญชีผู้ใช้ พร้อมอธิบายเพิ่มเติมว่า Claude Code ทำหน้าที่เป็นกลไกหลักในการปฏิบัติการ โดยจัดการการเรียกใช้เครื่องมือต่าง ๆ การรันคำสั่ง Bash การรักษาสถานะของเซสชัน และการทำงานหลายอย่างพร้อมกัน (Parallelization) ขณะที่ DeepSeek-v4-pro ทำหน้าที่เป็นโมเดลด้านการวิเคราะห์และตัดสินใจ รับผิดชอบการวางตรรกะของการโจมตี การสร้างสคริปต์ และการตัดสินใจในแต่ละขั้นตอน กล่าวโดยสรุปคือ ตรรกะของการโจมตีถูกประมวลผลผ่าน LLM ที่พัฒนาในจีน ส่วนการปฏิบัติการจริงอาศัยโครงสร้างการทำงานแบบเอเจนต์ (Agentic Execution) ของ Anthropic Claude Code

ข้อมูลอ้างอิง

Jul 16, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/07/daxin-resurfaces-in-taiwan-alongside.html