แจ้งเตือน

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 แคมเปญ CaptiveCrunch มุ่งเป้า Wi-Fi สาธารณะ ขโมยข้อมูลและติดตั้งมัลแวร์

วันที่แจ้งเตือน 6 สิงหาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้เผยแพร่รายงานภัยคุกคามทางไซเบอร์ กรณีแคมเปญ CaptiveCrunch มุ่งโจมตีผู้ใช้งาน Wi-Fi สาธารณะ (โรงแรมและสถานที่จัดงาน) เพื่อขโมยข้อมูลและติดตั้งมัลแวร์ โดย

การโจมตี	ผลกระทบ
ผู้ไม่หวังดีใช้เทคนิค Adversary-in-the-Middle (AiTM) เข้าควบคุมหรือแทรกแซงระบบ Captive Portal (หน้า Wi-Fi Login) ของเครือข่าย Wi-Fi สาธารณะ จากนั้นเปลี่ยนเส้นทางผู้ใช้งานไปยังเว็บไซต์ปลอม โดยมีรูปแบบสำคัญดังนี้: • ผู้ใช้งานเชื่อมต่อ Wi-Fi สาธารณะ (โรงแรมและสถานที่จัดงาน) • ถูกเปลี่ยนเส้นทางไปยังหน้าเว็บปลอม • แสดงข้อความให้อัปเดต Browser หรือระบบปฏิบัติการ • บางกรณีใช้เทคนิค ClickFix หลอกให้เปิด Command Prompt หรือ PowerShell และรันคำสั่งที่กำหนดเครื่องของเหยื่อ • ดาวน์โหลดและติดตั้งมัลแวร์ CornFlake โดยผู้ใช้งานไม่รู้ตัว	มัลแวร์ CornFlake ดำเนินการ: • ดักจับการพิมพ์แป้นพิมพ์ (Keylogging) • เข้าถึงไมโครโฟนและเว็บแคม • ขโมย Username/Password • ขโมย Session Cookies และ Access Tokens • ขโมยข้อมูลยืนยันตัวตนของ Microsoft 365 / Microsoft Entra ID เมื่อติดตั้งมัลแวร์สำเร็จ อาจส่งผลให้: • เครื่องคอมพิวเตอร์ถูกควบคุมจากระยะไกล • บัญชีผู้ใช้งานและรหัสผ่านรั่วไหล • ผู้ไม่หวังดีเข้าถึงอีเมล ไฟล์ และข้อมูลสำคัญขององค์กร • ถูกสวมรอยใช้งาน Microsoft 365 โดยไม่ต้องทราบรหัสผ่าน • ใช้เครื่องที่ถูกโจมตีเป็นจุดเริ่มต้นโจมตีระบบอื่นภายในองค์กร (Lateral Movement)
แนวทางการป้องกัน: • บังคับใช้งาน Always-on VPN หรือ Full Tunnel VPN เมื่อเชื่อมต่อเครือข่ายภายนอก • เปิดใช้งาน EDR/Endpoint Protection และ พิจารณาใช้ข้อมูลบ่งชี้การโจมตี (IoC) ที่เกี่ยวข้อง **(อ้างอิง 2)** • อัปเดตระบบปฏิบัติการและซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุด • ตรวจสอบ Sign-in Logs เพื่อค้นหาการเข้าสู่ระบบผิดปกติ • หากสงสัยว่าข้อมูล Credential รั่วไหล ให้ Revoke Session บังคับเปลี่ยนรหัสผ่าน และตรวจสอบบัญชีผู้ใช้ • อัปเดตเฟิร์มแวร์อุปกรณ์ Captive Portal และอุปกรณ์เครือข่ายอย่างสม่ำเสมอ • พิจารณาจำกัดหรือปิดการใช้ Device Code Authentication หากไม่จำเป็น	**คำแนะนำสำหรับผู้ใช้งาน:** • ดาวน์โหลดซอฟต์แวร์หรืออัปเดตจากเว็บไซต์ทางการเท่านั้น • เปิดใช้งาน Multi-Factor Authentication (MFA) • แจ้งผู้ดูแลระบบทันทีเมื่อพบพฤติกรรมผิดปกติ • หลีกเลี่ยงการดาวน์โหลดหรือติดตั้ง Browser Update หรือซอฟต์แวร์ที่แสดงผ่านหน้า Captive Portal หรือเว็บไซต์ที่ไม่น่าเชื่อถือ • หลีกเลี่ยงการรันคำสั่ง Command Prompt หรือ PowerShell ตามที่เว็บไซต์แนะนำ เว้นแต่ได้รับการยืนยันจากผู้ดูแลระบบ • หลีกเลี่ยงการป้อน Device Code หรือข้อมูลยืนยันตัวตนผ่านหน้าล็อกอินที่ไม่สามารถยืนยันความถูกต้องได้

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 6 ส.ค. 2569
2. https://www.microsoft.com/en-us/security/blog/2026/07/31/captivecrunch-midnight-blizzard-targets-travelers-worldwide-for-malware-delivery-and-credential-theft/?/