แคสเปอร์สกี้ แลป เผย “ShadowHammer” โจมตีแบบซัพพลายเชนทั่วโลก พบผู้ใช้ไทยโดนโจมตี 376 เครื่อง

แคสเปอร์สกี้ แลป เปิดเผยการค้นพบ “ShadowHammer” ปฏิบัติการ APT ล่าสุดที่กระทบผู้ใช้งานจำนวนมากโดยใช้วิธีการโจมตีซัพพลายเชน มีเป้าหมายโจมตีผู้ที่ใช้งาน ASUS Live Update Utility โดยอาชญากรไซเบอร์ได้แพร่มัลแวร์ผ่านทางแบ็กดอร์ช่วงเดือนมิถุนายนถึงพฤศจิกายนปีที่แล้ว ผู้เชี่ยวชาญคาดว่าจะมีผู้ใช้ที่ได้รับผลกระทบมากกว่าหนึ่งล้านรายทั่วโลก พบผู้ใช้ไทยจำนวน 376 รายถูกโจมตี

การโจมตีซัพพลายเชนเป็นหนึ่งในวิธีการที่อันตรายที่สุดและมีประสิทธิภาพที่สุด เริ่มแพร่ระบาดมากในปฏิบัติการโจมตีขั้นสูงในช่วง 2-3 ปีที่ผ่านมา อาทิ ShadowPad และ CCleaner ผู้ก่อการภายใต้ปฏิบัติการ “ShadowHammer” มีเป้าหมายเริ่มแพร่กระจายที่ ASUS Live Update Utility ซึ่งเป็นระบบที่ติดตั้งมาก่อนแล้ว (pre-installed) ในคอมพิวเตอร์เอซุสรุ่นใหม่ๆ สำหรับการอัปเดต BIOS UEFI ไดรเวอร์และแอปพลิเคชั่นอัตโนมัติ ผู้โจมตีได้แทรกแซงซอฟต์แวร์เอซุสรุ่นเก่าและแพร่กระจายโค้ดร้ายใส่ระบบ โดยที่มัลแวร์อัปเดตถูกเซ็นด้วย digital certicate และทำงานบนเซิร์ฟเวอร์ของเอซุส จึงสามารถหลีกเลี่ยงการถูกตรวจจับโดยโซลูชั่นรักษาความปลอดภัยของระบบได้

การค้นคว้ามัลแวร์ที่มีวิธีการและเทคนิคลักษณะใกล้เคียงกันนี้ ทำให้พบการแพร่กระจายในซอฟต์แวร์จากเวนเดอร์อื่นอีกสามรายในเอเชีย ซึ่งแคสเปอร์สกี้ แลป ได้รายงานการค้นพบนี้ไปยังเอซุสและเวนเดอร์อื่นแล้ว

นายวิทาลี คัมลัก ผู้อำนวยการทีมวิเคราะห์และวิจัยระดับโลก ของแคสเปอร์สกี้ แลป กล่าวว่า “มีเวนเดอร์หลายรายที่กลุ่มวายร้าย APT สนใจและต้องการหาประโยชน์จากฐานลูกค้าจำนวนมากของเวนเดอร์ ทั้งนี้จุดมุ่งหมายของผู้โจมตียังไม่ชัดเจนนัก และทีมนักวิจัยของเราก็ยังค้นหาว่าใครคือผู้อยู่เบื้องหลังการโจมตีนี้ อย่างไรก็ตาม เทคนิคและอ็อพเจ็คต่างๆ ที่ใช้ในการโจมตีชี้ว่าปฏิบัติการ ShadowHammer มีความเกี่ยวข้องกับ BARIUM APT ที่โยงไปถึงเหตุการณ์ ShadowPad และ CCleaner”

นายวิทาลีกล่าวเสริมว่า “แคสเปอร์สกี้ แลป ประเมินว่ามีผู้ใช้งานในประเทศไทยโดนโจมตีในปฏิบัติการนี้จำนวน 376 เครื่อง ซึ่งเป็นตัวเลขของ unique IP address ที่ได้ลงทะเบียนการติดตั้งแบ็กดอร์กับเอซุสไว้”

ผลิตภัณฑ์ทั้งหมดของแคสเปอร์สกี้ แลป สามารถตรวจจับและสกัดกั้นมัลแวร์ปฏิบัติการ “ShadowHammer” ได้อย่างมีประสิทธิภาพ และเพื่อป้องกันการตกเป็นเหยื่อจากการโจมตีแบบพุ่งไปยังเป้าหมายเจาะจง นักวิจัยของแคสเปอร์สกี้ แลป ขอแนะนำดังนี้

• นอกเหนือจากการป้องกันเอ็นพอยต์ที่จำเป็นต้องมี ขอแนะนำให้เพิ่มโซลูชั่นระดับองค์กรที่สามารถตรวจจับภัยคุกคามขั้นสูงในระดับเน็ตเวิร์กตั้งแต่แรกเริ่ม เช่น Kaspersky Anti Targeted Attack Platform

• สำหรับการตรวจจับระดับเอ็นพอยต์ การสอบสวนติดตาม และการฟื้นฟูความเสียหาย ขอแนะนำโซลูชั่นด้านการโต้ตอบต่อเหตุคุกคามหรืออีดีอาร์ เช่น Kaspersky Endpoint Detection and Response หรือติดต่อทีมผู้เชี่ยวชาญมืออาชีพด้านการโต้ตอบต่อเหตุคุกคาม

• นำข้อมูลภัยคุกคามอัจฉริยะหรือ Threat Intelligence ใส่ใน SIEM และตัวควบคุมความปลอดภัยอื่นๆ เพื่อให้เข้าถึงข้อมูลที่เกี่ยวข้องและทันสมัย และสามารถเตรียมการรับมือการโจมตีที่อาจเกิดขึ้นในอนาคตได้

ข้อมูลเพิ่มเติม https://securelist.com/operation-shadowhammer/89992/