วันที่ 4 กรกฎาคม 2568

สหรัฐฯ คว่ำบาตรผู้ให้บริการโฮสติ้ง Bulletproof ของรัสเซียที่สนับสนุนอาชญากรไซเบอร์ที่อยู่เบื้องหลังแรนซัมแวร์

สำนักงานควบคุมทรัพย์สินต่างประเทศ (OFAC) กระทรวงการคลังสหรัฐฯ ได้ประกาศคว่ำบาตร Aeza Group ผู้ให้บริการโฮสติ้งแบบ “Bulletproof Hosting (BPH)” จากรัสเซีย หลังตรวจพบว่าให้ความช่วยเหลืออาชญากรไซเบอร์ในการก่ออาชญากรรมและโจมตีเหยื่อทั้งในประเทศและทั่วโลก

การคว่ำบาตรครั้งนี้ยังขยายไปถึงบริษัทย่อยของ Aeza Group ได้แก่ Aeza International Ltd. (สาขาในสหราชอาณาจักร), Aeza Logistic LLC, Cloud Solutions LLC และบุคคลอีก 4 รายที่มีส่วนเกี่ยวข้องกับบริษัท ได้แก่:

- Arsenii Aleksandrovich Penzev: ซีอีโอและผู้ถือหุ้น 33% ของ Aeza Group
- Yurii Meruzhanovich Bozoyan: ผู้อำนวยการทั่วไปและผู้ถือหุ้น 33% ของ Aeza Group
- Vladimir Vyacheslavovich Gast: ผู้อำนวยการฝ่ายเทคนิคที่ทำงานใกล้ชิดกับ Penzev และ Bozoyan
- Igor Anatolyevich Knyazev: ผู้ถือหุ้น 33% ของ Aeza Group ที่ดูแลการดำเนินงานในช่วงที่ Penzev และ Bozoyan ไม่อยู่

นอกจากนี้ Penzev ถูกจับกุมเมื่อต้นเดือนเมษายน 2025 ในข้อหานำองค์กรอาชญากรรมและสนับสนุนการค้ายาเสพติดขนาดใหญ่ โดยให้บริการโฮสต์ BlackSprut ตลาดค้ายาเสพติดผิดกฎหมายบนดาร์กเว็บ ขณะที่ Bozoyan และพนักงาน Aeza อีกสองคน คือ Maxim Orel และ Tatyana Zubova ก็ถูกควบคุมตัวเช่นกัน

“อาชญากรไซเบอร์ยังคงพึ่งพาผู้ให้บริการ BPH อย่าง Aeza Group ในการอำนวยความสะดวกให้กับการโจมตีเรียกค่าไถ่, การขโมยเทคโนโลยีของสหรัฐฯ และการจำหน่ายยาเสพติดในตลาดมืด” Bradley T. Smith รักษาการปลัดกระทรวงการคลังด้านการก่อการร้ายและข่าวกรองทางการเงินกล่าว “กระทรวงการคลังสหรัฐฯ จะยังคงทำงานร่วมกับสหราชอาณาจักรและพันธมิตรระหว่างประเทศอย่างใกล้ชิด เพื่อเปิดโปงจุดสำคัญ โครงสร้างพื้นฐาน และบุคคลที่อยู่เบื้องหลังระบบของอาชญากรรมนี้”

ทำไม Bulletproof Hosting ถึงเป็นที่นิยมของอาชญากร?

บริการ BPH เป็นที่ชื่นชอบของอาชญากรไซเบอร์ เพราะมักเพิกเฉยต่อรายงานการละเมิดหรือคำขอปิดเว็บไซต์จากหน่วยงานบังคับใช้กฎหมาย และมักดำเนินธุรกิจในประเทศที่การบังคับใช้กฎหมายอ่อนแอหรือมีกฎหมายที่คลุมเครือโดยเจตนา ทำให้เป็นตัวเลือกที่ทนทานต่อการถูกรบกวนหรือถูกปิดลง สำหรับการโฮสต์โครงสร้างพื้นฐานอันตราย เช่น เว็บไซต์ฟิชชิ่ง และเซิร์ฟเวอร์สั่งการและควบคุม (C2)

สำนักงานใหญ่ของ Aeza Group ตั้งอยู่ที่เซนต์ปีเตอร์สเบิร์ก โดยถูกกล่าวหาว่าให้บริการแก่กลุ่มแรนซัมแวร์และมัลแวร์ประเภทขโมยข้อมูลหลายกลุ่ม เช่น BianLian, RedLine, Meduza และ Lumma ซึ่งบางกลุ่มถูกใช้โจมตีบริษัทด้านกลาโหม, เทคโนโลยีของสหรัฐฯ และเหยื่ออื่น ๆ ทั่วโลก

นอกจากนี้ รายงานที่เผยแพร่โดย Correctiv และ Qurium เมื่อเดือนกรกฎาคมปีก่อน ระบุว่าโครงสร้างพื้นฐานของ Aeza ถูกใช้โดยปฏิบัติการบงการข้อมูลที่หนุนรัสเซียในชื่อ Doppelganger อีกทั้งยังมีกลุ่ม Void Rabisu กลุ่มอาชญากรไซเบอร์ที่หนุนรัสเซียผู้อยู่เบื้องหลังมัลแวร์ RomCom RAT ที่ใช้บริการของ Aeza เช่นกัน

การเงินของ Aeza Group

ตามข้อมูลของ Chainalysis ที่อยู่กระเป๋าคริปโต TRON ที่เชื่อมโยงกับ Aeza Group ได้รับเงินมากกว่า 350,000 ดอลลาร์สหรัฐ ในรูปแบบคริปโต และถอนเงินไปยังที่อยู่ฝากในหลายแพลตฟอร์ม โดยที่อยู่ฝากเหล่านี้ยังได้รับเงินจากผู้ขายมัลแวร์ขโมยข้อมูลในตลาดมืด, Garantex และบริการเอสโครว์ที่ใช้ขายไอเทมบนแพลตฟอร์มเกมยอดนิยม

“ที่อยู่ที่ถูกระบุดูเหมือนจะทำหน้าที่เป็นกระเป๋าเงินสำหรับการจัดการทางการเงิน คอยถอนเงินจากตัวประมวลผลการจ่ายเงิน โอนเงินไปยังหลายแพลตฟอร์ม และบางครั้งก็รับชำระเงินโดยตรงสำหรับบริการของ Aeza” บริษัท Chainalysis ระบุ

ความพยายามต่อเนื่องในการปราบปรามอาชญากรรมไซเบอร์

ความเคลื่อนไหวนี้เกิดขึ้นหลังจากกระทรวงการคลังสหรัฐฯ เพิ่งประกาศคว่ำบาตรผู้ให้บริการ BPH รายอื่นจากรัสเซียชื่อ Zservers เมื่อราว 5 เดือนก่อน เนื่องจากมีส่วนอำนวยความสะดวกให้กับการโจมตีด้วยแรนซัมแวร์ เช่น กลุ่ม LockBit

เมื่อสัปดาห์ที่ผ่านมา Qurium ยังเชื่อมโยงผู้ให้บริการโฮสติ้งและพร็อกซี่เว็บของรัสเซียชื่อ Biterika กับการโจมตีแบบปฏิเสธการให้บริการ (DDoS) ต่อสื่ออิสระของรัสเซีย 2 แห่ง คือ IStories และ Verstka

มาตรการคว่ำบาตรเหล่านี้เป็นส่วนหนึ่งของความพยายามที่กว้างขึ้นในการทำลายห่วงโซ่อุปทานของแรนซัมแวร์ ด้วยการโจมตีไปที่ตัวแปรสำคัญ เช่น บริการโฮสติ้งที่เพิกเฉยต่อการร้องเรียน, เซิร์ฟเวอร์ C2 และโครงสร้างพื้นฐานบนดาร์กเว็บ เมื่ออาชญากรเปลี่ยนกลยุทธ์ การติดตามบริษัทที่ถูกคว่ำบาตร, คะแนนความน่าเชื่อถือของ IP และเครือข่ายที่ทนต่อการถูกร้องเรียน จึงกลายเป็นสิ่งสำคัญในงานวิเคราะห์ข่าวกรองภัยคุกคามสมัยใหม่

การคว่ำบาตร Aeza Group ของสหรัฐฯ เป็นการตอกย้ำความมุ่งมั่นในการปราบปรามอาชญากรรมไซเบอร์ที่อาศัยบริการ Bulletproof Hosting การตัดวงจรการสนับสนุนโครงสร้างพื้นฐานเหล่านี้ จะช่วยลดความสามารถของกลุ่มแฮกเกอร์ในการโจมตีและสร้างความเสียหายในวงกว้างได้อย่างมีนัยสำคัญ

ข้อมูลอ้างอิง

July 2, 2025 By Ravie Lakshmanan

- https://thehackernews.com/2025/07/us-sanctions-russian-bulletproof.html