ศูนย์ CSOC – Cyber Elite

Cyber Security Operation Center – Cyber Elite

วันที่ 25 มิถุนายน 2567

CDK Global **หยุดทำงานจากการโจมตีจาก** BlackSuit Ransomware

Executive Summary

ทางศูนย์ CSOC พบรายงานการแจ้งเตือนกี่ยวกับกลุ่ม BlackSuit Ransomware อยู่เบื้องหลังการหยุดทำงานของระบบ IT ขนาดใหญ่ของ CDK Global และการหยุดชะงักของธุรกิจตัวแทนจำหน่ายรถยนต์ทั่วทวีปอเมริกาเหนือ ตามข้อมูลจากหลายแหล่งที่มีความคุ้นเคยกับเหตุการณ์นี้แหล่งข้อมูลเดียวกัน ซึ่งให้ข้อมูลภายใต้เงื่อนไขการไม่เปิดเผยตัวตน CDK Global กำลังเจรจากับกลุ่ม BlackSuit Ransomware เพื่อรับตัวถอดรหัสและไม่ให้ข้อมูลที่ถูกขโมยถูกเปิดเผย การเจรจานี้เกิดขึ้นหลังจากการโจมตีของกลุ่ม BlackSuit Ransomware ทำให้ CDK ต้องปิดระบบ IT และศูนย์ข้อมูลของตนเพื่อป้องกันการแพร่กระจายของการโจมตี ซึ่งรวมถึงแพลตฟอร์มตัวแทนจำหน่ายรถยนต์ของบริษัทด้วย บริษัทพยายามกู้คืนการให้บริการเมื่อวันพุธที่ผ่านมา แต่ก็ประสบกับเหตุการณ์ความปลอดภัยทางไซเบอร์อีกครั้ง ทำให้ต้องปิดระบบ IT ทั้งหมดอีกครั้ง CDK เป็นผู้ให้บริการแพลตฟอร์ม Software-as-a-Service (SaaS) ที่ใช้ในการดำเนินงานทุกด้านของตัวแทนจำหน่ายรถยนต์ รวมถึงการขาย การเงิน สินค้าคงคลัง การบริการ และการทำงานในสำนักงานหลัง

เนื่องจากแพลตฟอร์มนี้ปิดตัวลง ตัวแทนจำหน่ายรถยนต์ต้องหันมาใช้กระดาษและปากกาในการดำเนินงาน โดยผู้ซื้อรถหลายรายบอกว่าพวกเขาไม่สามารถซื้อรถหรือรับบริการสำหรับรถที่มีอยู่ได้เนื่องจากการหยุดทำงานนี้บริษัทตัวแทนจำหน่ายรถยนต์รายใหญ่สองแห่ง ได้แก่ Penske Automotive Group และ Sonic Automotive เปิดเผยว่าพวกเขาก็ได้รับผลกระทบจากการหยุดทำงานนี้ ตัวแทนจำหน่ายทั้งหมดของบริษัทยังคงเปิดและดำเนินงานโดยใช้วิธีแก้ปัญหาชั่วคราวเพื่อลดผลกระทบที่เกิดจากการหยุดทำงานของ CDK

CDK ยังเตือนว่าผู้ก่อภัยคุกคามโทรหาตัวแทนจำหน่ายโดยอ้างเป็นตัวแทนหรือพันธมิตรของ CDK เพื่อเข้าถึงระบบโดยไม่ได้รับอนุญาต

ศูนย์ CSOC แนะนำให้ลูกค้าตรวจสอบรายละเอียดด้านความปลอดภัยของภายในองค์กรรวมถึงตรวจสอบความผิดปกติที่อาจเกิดขึ้นซึ่งเป็นความเสี่ยงที่อาจทำให้เกิดการโจมตีและเพื่อลดความเสี่ยงที่อาจเกิดขึ้น โดยเหตุการณ์นี้ก่อให้เกิดความเสี่ยงที่ยอมรับไม่ได้ต่อองค์กรควรต้องมีการดำเนินการตรวจสอบเพื่อลดความเสี่ยง

การแก้ไขปัญหา:

- ปิดระบบที่ได้รับผลกระทบทันทีถ้าพบการโจมตี ให้ปิดระบบเครือข่ายและอุปกรณ์ที่ได้รับผลกระทบเพื่อป้องกันการแพร่กระจายของ Ransomware ไปยังส่วนอื่นๆ ขององค์กร
- แจ้งเหตุการณ์ให้ทีม IT และผู้บริหารรับทราบทันทีเพื่อเริ่มต้นกระบวนการตอบสนองต่อเหตุการณ์
- ตรวจสอบและระบุแหล่งที่มาทำการตรวจสอบและระบุว่า Ransomware เข้าสู่ระบบได้อย่างไรเพื่อป้องกันเหตุการณ์ซ้ำรอยในอนาคต

ข้อมูลอ้างอิง

- https://www.bleepingcomputer.com/news/security/cdk-global-outage-caused-by-blacksuit-ransomware-attack/