ประจำวันพฤหัสบดีที่ 9 มิถุนายน 2565

แรนซัมแวร์ Black Basta รองรับการเข้ารหัสเซิร์ฟเวอร์ VMware ESXi ได้แล้ว

แก๊งแรนซัมแวร์ Black Basta ใช้คุณลักษณะใหม่ในการเข้ารหัสเครื่องเสมือน VMware ESXi (VMs) ที่ทำงานบนเซิร์ฟเวอร์ Linux โดยนักวิจัยจาก Uptycs ได้รายงานการค้นพบแรนซัมแวร์ Black Basta ตัวใหม่ที่รองรับการเข้ารหัสเซิร์ฟเวอร์ VMWare ESXi การย้ายครั้งนี้มีจุดมุ่งหมายเพื่อขยายเป้าหมายที่เป็นไปได้ การรองรับ VMware ESXi ได้ถูกนำมาใช้โดยกลุ่มแรนซัมแวร์หลายตระกูลแล้ว รวมถึง LockBit , HelloKitty , BlackMatter และ Revil ซึ่ง Black Basta เปิดใช้งานตั้งแต่เดือนเมษายน พ.ศ. 2565 เช่นเดียวกับการดำเนินการแรนซัมแวร์อื่น ๆ ที่ใช้รูปแบบการโจมตีแบบ double-extortion attack แรนซัมแวร์จะผนวกนามสกุล .basta เข้ากับชื่อไฟล์ที่เข้ารหัส และสร้างบันทึกค่าไถ่ชื่อ readme.txt ในแต่ละโฟลเดอร์

เมื่อเร็วๆ นี้ นักวิจัยจากกลุ่ม NCC พบความร่วมมือครั้งใหม่ในภัยคุกคามระหว่างกลุ่มแรนซัมแวร์ Black Basta และการทำงานของมัลแวร์ Qbot นักวิจัยของ NCC Group ค้นพบความร่วมมือครั้งใหม่ในขณะที่กำลังสืบสวนเหตุการณ์ที่เกิดขึ้นเมื่อเร็วๆ นี้ ซึ่งแตกต่างจากความร่วมมือในอดีตที่กลุ่ม Black Basta ใช้ QBot เพื่อกระจายไปทั่วทั้งเครือข่ายเป้าหมาย

ที่มาของข่าว : https://securityaffairs.co/wordpress/132037/hacking/black-basta-ransomware-vmware-esxi.html