แคสเปอร์สกี้ แลป เผย แบงกิ้งโทรจัน RTM ลุยโจมตีกลุ่มธุรกิจไปแล้วมากกว่า 130,000 ราย

นักวิจัยของแคสเปอร์สกี้ แลปตรวจพบกิจกรรมของโทรจัน RTM Banking Trojan พบยูสเซอร์ถูกโจมตีในปี 2018 ที่ผ่านมามากกว่า 130,000 เพิ่มขึ้นจากปี 2017 ที่มีผู้ถูกโจมตีเพียง 2,376 ราย และมีแนวโน้มการโจมตีอย่างต่อเนื่องในปีนี้ พบยูสเซอร์มากกว่า 30,000 รายถูกโจมตีตั้งแต่ต้นปี 2019 เป็นต้นมา ทำให้ RTM กลายเป็นโทรจันที่แอคทีฟที่สุดในกลุ่มแบงกิ้ง

แบงกิ้งโทรจันจัดเป็นภัยไซเบอร์ที่สร้างความเสียหายมากที่สุดเพราะออกแบบมาเพื่อโจมตีบัญชีการเงินและทรัพย์สิน เริ่มต้นด้วยการขโมยข้อมูลล็อคอิน เพื่อแอบส่องเซสชั่นธุรกรรมการเงินทางออนไลน์ จากนั้นปลอมแฝงตัวเข้าแทนที่รายละเอียดเวลาที่เหยื่อทำธุรกรรมการเงิน ชำระเงิน โอนเงิน หรือแม้แต่ขโมยเงินเอาดื้อๆ ด้วยการใช้รีโมทแอคเซสทูลบังคับมาจากระยะไกล มัลแวร์มีเป้าหมายที่เจ้าหน้าที่การเงินในบริษัทเล็กและกลาง ในเซ็คชั่นไอทีและกฎหมาย โทรจัน RTM จึงกลายเป็นส่วนหนึ่งของเทรนด์ทั่วไปซึ่งอาชญากรไซเบอร์ไม่ค่อยสนใจบริษัทด้านการเงินแล้ว แต่หันมาสนใจภาคเอกชนซึ่งส่วนมากแล้วไม่ค่อยได้ลงทุนไปกับโซลูชั่นเพื่อการป้องกันความมั่นคงและปลอดภัยขององค์กร เท่าที่เห็นตอนนี้ ส่วนมากโทรจันจะโจมตีบริษัทที่อยู่ในรัสเซีย

โทรจัน RTM แพร่กระจายผ่านอีเมลฟิชชิ่ง ปลอมแปลงข้อความเกี่ยวกับการเงินบัญชี พร้อมมีลิ้งก์และไฟล์แนบ เมื่อมัลแวร์หาทางติดตั้งตัวเองลงบนเครื่องของเหยื่อได้แล้ว ผู้ร้ายไซเบอร์ก็จะมีช่องทางในการเข้าควบคุมระบบที่ติดเชื้อนั้นได้ทั้งหมด

แคสเปอร์สกี้ แลป ได้ประมาณความเสียหายในช่วงสองปีที่ผ่านมาคิดเป็นมูลค่าหลายล้านรูเบิ้ล (หรือประมาณ 15,104 เหรียญสหรัฐ) ต่อหนึ่งทรานส์แอคชั่นเลยทีเดียว

นายเซอร์เกย์ โกลอฟวานอฟ นักวิจัยด้านระบบความปลอดภัย แคสเปอร์สกี้ แลป กล่าวว่า “ตอนนี้แน่ชัดแล้วว่าว่ามีหลายกรณีที่การโจมตีไซเบอร์เริ่มขึ้นก่อนที่รัสเซียแล้วค่อยขยายตัวไปยังประเทศอื่น แบงกิ้งโทรจันที่ชื่อ RTM ตัวนี้เป็นตัวอย่างของแนววิวัฒนาการของตัวมัน จึงขอเชิญชวนกระตุ้นให้องค์กรต่างๆ ที่มีโอกาสจะเป็นเป้าหมายของมัลแวร์ชนิดนี้ ให้เร่งดำเนินการป้องกัน ใช้มาตรการจัดหาโซลูชั่นเพื่อตรวจเช็คและสกัดกั้นภัยไซเบอร์ตัวนี้”

ผู้เชี่ยวชาญเฉพาะทางของแคสเปอร์สกี้ แลป ขอแนะนำวิธีการเพื่อเป็นการป้องกันธุรกิจของคุณจากมัลแวร์การเงินรวมทั้งโทรจัน RTM ดังต่อไปนี้:

- อบรมพนักงาน เจ้าหน้าที่ในองค์กร โดยเฉพาะส่วนงานที่เกี่ยวข้องกับการเงินการบัญชี เพื่อให้มีความรู้เท่าทันการโจมตีแบบฟิชชิ่ง
- ติดตั้งแพทช์เวอร์ชั่นล่าสุดของซอฟต์แวร์ที่ใช้งานทุกตัว
- ห้ามติดตั้งโปรแกรมจากแหล่งที่คุณไม่รู้จักโดยเด็ดขาด
- ใช้โซลูชั่นเพื่อความปลอดภัยที่มีประสิทธิภาพสำหรับธุรกิจโดยเฉพาะ แบบที่มีฟีเจอร์วิเคราะห์พฤติกรรม เช่น โซลูชั่น Kaspersky Endpoint Security for Business