# แจ้งเตือน! แคสเปอร์สกี้พบไทยตกเป็นเหยื่อแคมเปญการโจมตีโรงแรมทั่วโลก ฉกข้อมูลบัตรเครดิตลูกค้า


แคสเปอร์สกี้ตรวจพบแคมเปญการโจมตีชื่อ “RevengeHotels” หรือ รีเวนจ์โฮเต็ลส์ โดยมุ่งโจมตีธุรกิจการโรงแรม นักวิจัยได้พบและยืนยันแล้วว่ามีโรงแรมมากกว่า 20 แห่งในทวีปละตินอเมริกา ยุโรปและเอเชียได้กลายเป็นเหยื่อของการโจมตีของมัลแวร์แบบมีเป้าหมาย พบว่ามีโรงแรมในประเทศไทยตกเป็นเหยื่อด้วย และยังมีแนวโน้มว่าโรงแรมทั่วโลกอีกหลายแห่งก็กำลังตกเป็นเหยื่อเช่นกัน ข้อมูลบัตรเครดิตของผู้เดินทางที่ถูกเก็บเอาไว้ในระบบของโรงแรม รวมทั้งข้อมูลที่ได้รับมาจากตัวแทนท่องเที่ยวออนไลน์ (OTAs) ต่างตกในความเสี่ยงถูกโจรกรรมเพื่อนำมาปล่อยขายต่อให้อาชญากรไซเบอร์ทั่วโลก

RevengeHotels คือ แคมเปญที่ประกอบขึ้นด้วยหลากหลายกลุ่มที่ใช้ Remote Access Trojans (RATs) แบบดั้งเดิมในการปล่อยเชื้อเข้าสู่ธุรกิจการโรงแรม โดยเริ่มออกก่อกวนมาตั้งแต่ปี 2015 แต่มาพบเห็นมากขึ้นในปี 2019 อย่างน้อยก็มีสองกลุ่ม คือ RevengeHotels และ ProCC ที่ถูกตรวจพบว่าเป็นส่วนของแคมเปญนี้ อย่างไรก็ตาม น่าจะมีกลุ่มอาชญากรไซเบอร์มากกว่านี้ที่มีส่วนเกี่ยวข้องในการกระทำการ

แกนหลักของการโจมตีที่แคมเปญนี้ใช้คือ อีเมลที่มาพร้อมเอกสารแนบ ไม่ว่าจะเป็น Word, Excel หรือ PDF ที่

ปลอมแปลงมาอย่างดี บางไฟล์ก็จะใช้ CVE-2017-0199 โหลดเข้ามาโดยใช้ VBS และ PowerShell scripts และจากนั้นก็จะติดตั้ง RATs ที่มีการปรับแต่งมากมายหลายเวอร์ชั่น รวมทั้งมัลแวร์ที่ปรับแต่งขึ้นมา เช่น ProCC บนเครื่องของเหยื่อที่สามารถรันคอมมานด์นั้นได้ และเซ็ตอัพการเข้าถึงระยะไกลเข้าไปยังระบบที่ติดเชื้อ

อีเมลที่เป็นสเปียร์ฟิชชิ่งถูกร่างขึ้นมาเป็นพิเศษเพื่อให้มีรายละเอียดเฉพาะตัว และทำให้ดูเหมือนบุคคลที่มีอยู่จริงในองค์กรนั้นๆ ทำทีเป็นออกบุ๊กกิ้งโรงแรมสำหรับกลุ่มทัวร์ขนาดใหญ่ สำหรับคนหลายคน เป็นที่น่าสังเกตว่าแม้จะระวังเท่าใด ก็ยังมีคนหลงเปิดอีเมลและคลิ้กเปิดไฟล์นั้นจนได้ เพราะดูเหมือนอีเมลของจริงมาก เต็มไปรายละเอียดมากมายที่น่าเชื่อถือ (เช่น สำเนาเอกสารที่ออกโดยราชการ และเหตุผลที่จองโรงแรม เป็นต้น) จุดสังเกตุที่เล็ดลอดออกมาให้เราจับได้น่าจะเป็นการพิมพ์ชื่อโดเมนของบริษัทและองค์กรผิด

เมื่อคอมพิวเตอร์ตกเป็นเหยื่อก็จะถูกใช้งานจากระยะไกล จากหลักฐานที่นักวิจัยของแคสเปอร์สกี้รวบรวมได้ชี้ว่า มีนำเอาข้อมูลจากคอมพิวเตอร์ของแผนกต้อนรับไปขายต่อในฟอรั่มใต้ดินที่มีสมาชิกคอยซื้อข้อมูลลักษณะแบบนี้อีกต่อหนึ่ง มัลแวร์จะทำการรวบรวมข้อมูลจากคลิปบอร์ดในคอมพิวเตอร์ เอกสารที่สั่งพิมพ์ออกทางเครื่องพิมพ์ รวมถึงหน้าจอสกรีนช็อต (ฟังก์ชั่นนี้จะถูกกระตุ้นด้วยคำเฉพาะในภาษาอังกฤษหรือโปรตุกีส) เนื่องจากพนักงานโรงแรมมักจะเก็บข้อมูลบัตรเครดิตของลูกค้าจากตัวแทนท่องเที่ยวออนไลน์เพื่อใช้งาน และนับเป็นจุดอ่อนที่อาชญากรเหล่านี้ใช้ฉวยโอกาสได้

เครื่องตรวจวัดระยะไกลของแคสเปอร์สกี้ยืนยันว่าเป้าหมายอยู่ที่อาร์เจนตินา โบลิเวีย บราซิล ชิลี คอสตาริกา ฝรั่งเศส อิตาลี เม็กซิโก โปรตุเกส สเปน ตุรกี และประเทศไทย อย่างไรก็ตามจากข้อมูลที่ตัดมาจาก Bit.ly บริการย่อลิ้งก์ยอดฮิตที่พวกผู้ร้ายไซเบอร์นิยมใช้ในการแพร่กระจายลิ้งก์ของตัว นักวิจัยแคสเปอร์สกี้คาดว่ายูสเซอร์จากหลายประเทศอย่างน้อยก็ต้องเคยคลิ้กเข้าไปตามลิ้งก์เหล่านี้ หมายความว่าจะต้องมีจำนวนเหยื่อมากกว่านี้ในอีกหลายประเทศ

ดิมิทรี่ เบสทุซเชฟ หัวหน้าทีมวิเคราะห์และวิจัย (Global Research and Analysis Team – GReAT) แคสเปอร์สกี้ภูมิภาคละตินอเมริกา กล่าวว่า “ขณะที่ยูสเซอร์ต่างกังวลว่าการป้องกันข้อมูลของตนเพียงพอไหม พวกผู้ร้ายไซเบอร์ก็มุ่งไปโจมตีธุรกิจขนาดเล็ก ซึ่งมักไม่ค่อยจะมีความแข็งแกร่งในการป้องกันตัวเองเท่าใดนัก แถมยังมีข้อมูลส่วนตัวอยู่มากมายให้ผู้ร้ายเข้าไปขโมยอีกด้วย ผู้ประกอบการโรงแรมและธุรกิจขนาดเล็กที่ติดต่อกับลูกค้าและมีข้อมูลของลูกค้าอยู่ จึงจำเป็นอย่างยิ่งที่จะต้องเพิ่มความระมัดระวัง และติดตั้งใช้โซลูชั่นเพื่อความปลอดภัยระดับสูงเพื่อกันเหตุการณ์ข้อมูลรั่วไหลที่อาจเกิดขึ้นได้ นอกจากเป็นการทำร้ายลูกค้าแล้ว ยังทำลายชื่อเสียงของโรงแรมและธุรกิจอีกด้วย”

“ประเทศไทยเป็นแหล่งท่องเที่ยวยอดนิยมแห่งหนึ่งของโลก มีตัวเลือกมากมายจึงดึงดูดใจทั้งนักท่องเที่ยวและอาชญากรไซเบอร์ในการเลือกเหยื่อโจมตี เป้าหมายของแคมเปญนี้คือการขโมยข้อมูลบัตรเครดิตให้ได้มากที่สุด ผู้ร้ายไซเบอร์จึงมักเลือกโรงแรมชื่อดังที่มีลูกค้าเข้าพักจำนวนมาก ยิ่งเลือกโรงแรมหรูหราก็ยิ่งมีโอกาสได้ข้อมูลบัตร

เครดิตของลูกค้าฐานะดีประวัติดีอีกด้วย แคสเปอร์สกี้ตรวจพบและยืนยันว่า มีโรงแรมหนึ่งแห่งในไทยที่ได้รับอีเมลโจมตีจริง แต่ยังไม่แน่ชัดว่าเป็นเหยื่อของแคมเปญนี้หรือไม่ อีกทั้งไม่สามารถยืนยันได้ว่ามีโรงแรมอื่นที่ตกเป็นเหยื่อลักษณะนี้อีกหรือไม่ แต่ทั้งหมดนี้ก็มีเหตุผลให้เชื่อได้เช่นกัน” ดิมิทรี่กล่าวเสริม

คำแนะนำเพื่อความปลอดภัยสำหรับนักท่องเที่ยว:
– ใช้บัตรเครดิตเสมือนจริง (virtual payment card) ในการจองตั๋ว จองที่พัก หรือทำธุรกรรมผ่านตัวแทนท่องเที่ยว เพราะบัตรจะใช้งานได้เพียงครั้งเดียวเท่านั้น และจะหมดอายุไม่สามารถใช้งานได้อีก
– เมื่อชำระเงินค่าจองหรือเช็คเอ้าท์ที่โรงแรมที่พัก ให้ใช้ virtual wallet เช่น Apple Pay หรือ Google Pay หรือบัตรเครดิตสำรองที่มีการจำกัดวงเงิน

เจ้าของหรือผู้บริหารโรงแรมควรมีมาตรการเหล่านี้เพื่อความปลอดภัยต่อข้อมูลของลูกค้าผู้เข้าพัก:
– ประเมินความเสี่ยงของนระบบเครือข่ายที่ใช้งาน และติดตั้งกฎระเบียบในการจัดการข้อมูลของลูกค้า
– ใช้โซลูชั่นเพื่อความปลอดภัยที่ไว้ใจได้ ที่มีฟีเจอร์ป้องกันเมื่อใช้เว็บไซต์และควบคุมจัดการแอปพลิเคชั่น อย่างเช่น Kaspersky Endpoint Security for Business ฟีเจอร์การป้องกันเว็บ (Web protection) ช่วยบล็อกการเข้าเว็บไซต์ที่อาจเป็นฟิชชิ่งหรือมีเชื้อมัลแวร์ ขณะที่ฟีเจอร์แอปพลิเคชั่นคอนโทรล (ในโหมด white list) คอยตรวจดูแอปพลิเคชั่นเฉพาะที่อยู่ในรายการเท่านั้นที่สามารถเปิดใช้งานได้บนคอมพิวเตอร์ของโรงแรมได้
– อบรมให้พนักงานมีความรู้ด้านความปลอดภัยไซเบอร์ ให้สามารถระบุสเปียร์ฟิชชิ่ง ระวังตัวเวลาที่ใช้อีเมล เป็นต้น

ท่านสามารถอ่านรายงานเรื่อง “RevengeHotels: cybercrime targeting hotel desks worldwide” ได้ที่ https://securelist.com/revengehotels/95229/