มัลแวร์โจมตีตู้เอทีเอ็มขยายตัวอย่างต่อเนื่องข้อมูลจาก TrendLabs Security Intelligence Blog

มัลแวร์โจมตีตู้เอทีเอ็มขยายตัวอย่างต่อเนื่อง
ข้อมูลจาก TrendLabs Security Intelligence Blog
โดย เดวิด แซนชู และนอร์แมนน์ ฮัก (นักวิจัยอาวุโสด้านภัยคุกคาม)

เครื่องรับจ่ายเงินอัตโนมัติ (เอทีเอ็ม) นอกจากจะต้องเผชิญกับคนร้ายที่พยายามงัดแงะตัวเครื่องแล้ว ยังต้องรับมือกับการโจมตีทางคอมพิวเตอร์ที่เรียกว่า ‘มัลแวร์เอทีเอ็ม’ ที่วงการอุตสาหกรรมด้านความปลอดภัยและผู้รักษากฎหมายเริ่มค้นพบว่า ‘มัลแวร์เอทีเอ็ม’ เป็นภยันตรายรูปแบบใหม่ ซึ่งถูกสร้างขึ้นเพื่อมุ่งโจมตีระบบตู้เอทีเอ็มโดยเฉพาะ ซึ่งถูกตรวจจับได้เมื่อไม่กี่ปีที่ผ่านมาและเป็นการโจมตีที่ประสบความสำเร็จ การเปลี่ยนแปลงรูปแบบการโจมตีไปสู่ช่องทางดิจิตอลนี้แสดงให้เห็นว่ากลุ่มคนร้ายรู้วิธีในการใช้มัลแวร์เพื่อขโมยเงินและข้อมูลบัตรจากตู้เอทีเอ็มซึ่งเหล่าคนร้ายพบว่าเป็นวิธีการที่ง่ายและปลอดภัยสำหรับพวกเขามากกว่า การโจมตีผ่านช่องทางดิจิตอลมีแนวโน้มที่จะขยายตัวอย่างต่อเนื่องในอนาคต และจำเป็นอย่างยิ่งที่เราควรตระหนักถึงช่องทางการโจมตีในรูปแบบต่างๆ ที่คนร้ายสร้างขึ้นเพื่อก่ออาชญากรรม

รูปที่ 1. สถิติการโจมตีเครื่องเอทีเอ็มในยุโรปตั้งแต่ปี 2554 ถึง 2558

การปลอมแปลงและการโจมตีทางกายภาพต่อเครื่องเอทีเอ็ม
สถิติข้างต้นแสดงให้เห็นถึงการเพิ่มขึ้นของการโจมตีเครื่องเอทีเอ็มด้วยวิธีการปลอมแปลงบัตรในช่วงปีที่ผ่านมา (เพิ่มขึ้น 15% จากปี 2557 ถึง 2558) นอกจากนี้ แนวโน้มการเพิ่มขึ้นของการโจมตีด้วยซอฟต์แวร์ในทุกส่วนยังชี้ให้เห็นว่ากลุ่มคนร้ายที่มีความเชี่ยวชาญสูงได้มองเห็นโอกาสแฝงในชุดเครื่องมือสำหรับการโจมตีซึ่งสามารถนำมาใช้กับระบบเอทีเอ็มได้ สถิติดังกล่าวชี้ให้เห็นถึงจุดเริ่มต้นของการใช้มัลแวร์เพื่อเจาะระบบเอทีเอ็ม แต่แน่นอนว่าแนวโน้มนี้จะยังคงดำเนินต่อไปในอนาคต

ถึงแม้ว่าจะยังไม่มีสถิติการโจมตีของมัลแวร์เอทีเอ็มในสหรัฐฯ แต่ ทีมงานฝ่ายรักษาความปลอดภัยระบบเอทีเอ็มของยุโรป ระบุว่า “มีการรายงานความสูญเสียที่เกิดขึ้นใน 53 ประเทศนอกเขตพื้นที่ที่ใช้ระบบ Single Euro Payments Area (SEPA) และใน 10 ประเทศที่ใช้ระบบ SEPA ประเทศที่เกิดความสูญเสียดังกล่าวมากที่สุด 3 ประเทศ ได้แก่ สหรัฐฯ อินโดนีเซีย และฟิลิปปินส์”

ผลกระทบจากการแพร่กระจายของมัลแวร์เอทีเอ็ม
เทรนด์ ไมโคร และศูนย์อาชญากรรมไซเบอร์แห่งยุโรป (European Cybercrime Center – EC3) ของยูโรโพล (Europol) ได้ทำงานร่วมกันเพื่อตรวจสอบภัยคุกคามที่มุ่งโจมตีระบบเอทีเอ็ม ผลการวิจัยชี้ให้เห็นว่ามีปัจจัยมากมายที่ผลักดันการเปลี่ยนแปลงไปสู่การใช้ชุดเครื่องมือแฮ็กระบบเครื่องเอทีเอ็มเป้าหมายไว้ควบคู่ไปกับวิธีการโจมตีแบบเดิมๆ มากขึ้น
ปัจจัยสำคัญประการหนึ่งคือ การใช้ระบบปฏิบัติการ (OS) ที่ล้าสมัย เช่น Windows XP®
ซึ่งไม่สามารถติดตั้งแพทช์ด้านความปลอดภัยได้อีกต่อไป อีกเหตุผลหนึ่งคือ กลุ่มอาชญากร
มีเทคโนโลยีที่ทันสมัยมากขึ้นและเริ่มรู้แล้วว่าช่องทางดิจิตอลมีความเสี่ยงน้อยกว่า ทั้งยังเปิดโอกาสให้สามารถเคลื่อนย้ายเงินและปกปิดซ่อนเร้นเพื่อหลบหลีกการจับกุมได้ง่ายกว่า ปัจจัยที่สำคัญอีกอย่างหนึ่งก็คือ ผู้จำหน่ายเครื่องเอทีเอ็มตัดสินใจที่จะใช้มิดเดิลแวร์ที่มี Application Programming Interface (API) เพื่อสื่อสารกับอุปกรณ์ต่อพ่วงของเครื่อง (เช่น แป้นกดรหัส เครื่องจ่ายเงินสด ฯลฯ) โดยไม่สนใจว่าจะเป็นรุ่นใด มิดเดิลแวร์ที่ว่านี้คือ มิดเดิลแวร์ eXtensions for Financial Services (XFS) วิธีการง่ายๆ ก็คือ ให้ลองจินตนาการว่าเครื่องเอทีเอ็มที่ทันสมัยก็เป็นเหมือนเครื่องพีซีที่ใช้ระบบ MS Windows® ที่มีกล่องเก็บเงินติดอยู่
กับเครื่องและถูกควบคุมด้วยซอฟต์แวร์ จะทำให้เข้าใจได้ง่ายว่าเครื่องเอทีเอ็มตกเป็นเป้าหมายการโจมตีของผู้สร้างมัลแวร์ได้อย่างไร

รูปที่ 2. สถาปัตยกรรมระบบ XFS
ตระกูลหลักๆ ของมัลแวร์เอทีเอ็มที่มีอยู่
งานวิจัยร่วมกันระหว่างเทรนด์ ไมโครกับศูนย์ European Cybercrime Center (EC3) ของ Europol ยังสำรวจตรวจสอบประเภทหลักๆ ของมัลแวร์ที่แพร่กระจายในปัจจุบัน แผนผังข้างต้นเผยให้เห็นรูปแบบที่น่าสนใจเกี่ยวกับจุดเริ่มต้นของโค้ด ธนาคารพาณิชย์ในละตินอเมริกาและยุโรปตะวันออกไม่ได้ดำเนินมาตรการรักษาความปลอดภัยที่เพียงพอ จึงเปิดโอกาสให้อาชญากรเข้าโจมตีเครื่องเอทีเอ็มในภูมิภาคดังกล่าว แม้ว่าการโจมตีจะเป็นไปอย่างช้าๆ แต่เราก็พบว่ามีการส่งต่อเทคนิคเหล่านี้ไปยังภูมิภาคอื่นๆ ถึงแม้เรายังไม่พบว่ามีการซื้อขายมัลแวร์เอทีเอ็มในตลาดมืด แต่เราคาดว่าจะเกิดขึ้นในอนาคตอันใกล้อย่างแน่นอน

มัลแวร์แต่ละตระกูลที่ระบุไว้ข้างต้นมีลักษณะที่แตกต่างกัน 2 ส่วนหลักๆ คือ 1) ประเภทของผู้ผลิตเครื่องเอทีเอ็ม และ 2) ความสามารถที่เฉพาะเจาะจงของมัลแวร์ เช่น ใช้สำหรับขโมยข้อมูลที่ผู้ใช้ป้อนเข้าเครื่อง เช่น หมายเลขบัตรและรหัส PIN หรือใช้สำหรับจ่ายเงินสดออก
จากตู้ สิ่งที่มัลแวร์เหล่านี้มีเหมือนกันก็คือ จะต้องทำการติดตั้งผ่านทาง USB หรือซีดีไดรฟ์

รูปที่ 3. มัลแวร์เอทีเอ็มในตระกูลต่างๆ และแหล่งกำเนิดทางภูมิศาสตร์

ข้อมูลที่พบนี้อ้างอิงการตรวจสอบที่เทรนด์ ไมโครและศูนย์ European Cybercrime Center (EC3) ของ Europol

ได้ทำงานร่วมกัน ในการตรวจสอบสถานะปัจจุบันของมัลแวร์เอทีเอ็ม ผลลัพธ์ที่ได้คือเอกสารรายงานที่เน้นให้เห็นถึงภัยคุกคามทางไซเบอร์ที่มีการพัฒนาอย่างต่อเนื่องโดยพุ่งเป้าไปที่เครื่องเอทีเอ็ม นอกจากนี้ยังมีข้อมูลวิเคราะห์เกี่ยวกับวิธีการใหม่ๆ
ที่แฮ็กเกอร์ใช้ รวมถึงแนวทางป้องกันที่สำคัญๆ ให้กับองค์กรที่ต้องการปกป้องธุรกิจและลูกค้า รายงานที่จัดทำร่วมกันนี้นับเป็นอีกหนึ่งตัวอย่างของความร่วมมือที่ประสบความสำเร็จระหว่างหน่วยงานบังคับใช้กฎหมายกับภาคอุตสาหกรรมในการต่อสู้กับอาชญากรรมทางคอมพิวเตอร์

คุณสามารถอ่านข่าวประชาสัมพันธ์ได้ที่นี่

เกี่ยวกับ เทรนด์ ไมโคร
เทรนด์ ไมโคร อินคอร์ปอเรทเต็ด ผู้นำระดับโลกด้านซอฟต์แวร์ความปลอดภัย มุ่งมั่นที่จะสร้างโลกที่ปลอดภัยสำหรับการแลกเปลี่ยนข้อมูลดิจิตอล จากประสบการณ์มากกว่า 27 ปีของเรา โซลูชั่นของเราได้ให้บริการทั้งสำหรับผู้ใช้ทั่วไป องค์กรธุรกิจ และหน่วยงานภาครัฐ โดยนำเสนอระบบรักษาความปลอดภัยแบบหลายระดับขั้นการปกป้องในอุปกรณ์พกพา อุปกรณ์ลูกข่าย เกตเวย์ เซิร์ฟเวอร์ และระบบคลาวด์ เทรนด์ ไมโคร ช่วยปกป้องข้อมูลอย่างชาญฉลาด ด้วยเทคโนโลยีด้านความปลอดภัยที่ก้าวล้ำ ใช้งานและบริหารจัดการง่าย มีการพัฒนาเพื่อรองรับเทคโนโลยีใหม่ๆ อย่างไม่หยุดนิ่ง โซลูชั่นทั้งหมดของเราขับเคลื่อนด้วย ระบบวิเคราะห์และเฝ้าระวังภัยคุกคามระดับโลกแบบออนไลน์ ซึ่งเป็นโครงสร้างพื้นฐาน Trend Micro™ Smart Protection Network™ ที่พร้อมสนับสนุนลูกค้าด้วยผู้เชี่ยวชาญด้านภัยคุกคามกว่า 1,200 คนทั่วโลก ดูข้อมูลเพิ่มเติมได้ที่ www.trendmicro.co.th