เตือนภัย “เจเนซิส (Genesis)” ร้านออนไลน์ใต้ดินสุดอันตราย จำหน่ายอัตลักษณ์ดิจิทัลปลอมนับหมื่นรหัสเพื่อหลบเลี่ยงโปรแกรมป้องกันการทุจริต

แคสเปอร์สกี แล็บ ตีพิมพ์ผลการตรวจสอบเกี่ยวกับ “เจเนซิส (Genesis)” ร้านค้าออนไลน์ที่ทำการซื้อขายอัตลักษณ์ดิจิทัลทั้งที่โจรกรรมมาและที่ถูกกฎหมายมากกว่า 60,000 รหัส ทำให้การทุจริตบัตรเครดิตสามารถกระทำได้ง่ายขึ้น โดยตลาดแห่งนี้และเครื่องมือผิดกฎหมายอื่น ๆ มีความเกี่ยวพันกับการละเมิดการทำงานของระบบป้องกันการทุจริตจากการเรียนรู้ของเครื่อง (Machine-learning) ที่เรียกว่าหน้ากากดิจิทัล (Digital Mask) ซึ่งเป็นการเก็บประวัติบุคคลที่เชื่อถือได้ด้วยหลักเกณฑ์การจดจำอุปกรณ์ที่รู้จักและรูปแบบพฤติกรรมของลูกค้า

ทุกครั้งที่เรากรอกข้อมูลทางการเงิน การชำระเงิน และข้อมูลส่วนตัวในการทำธุรกรรมออนไลน์ โซลูชั่นป้องกันการทุจริตจากการเรียนรู้เชิงวิเคราะห์ขั้นสูง จะทำการเปรียบเทียบความสอดคล้องของเรากับสิ่งที่เรียกว่าหน้ากากดิจิทัล โดยหน้ากากเหล่านี้จะมีลักษณะเฉพาะสำหรับผู้ใช้งานแต่ละราย และทำงานร่วมกับลายนิ้วมือบนอุปกรณ์และเบราว์เซอร์ที่ถูกใช้เป็นประจำในการชำระเงิน/ธนาคารออนไลน์ (เช่น ข้อมูลบนหน้าจอและระบบปฏิบัติการ ขอบเขตของข้อมูลเบราว์เซอร์ เช่น ตัวนำหน้า เขตเวลา ปลั๊กอินที่ติดตั้ง ขนาดการรับ-ส่งข้อมูล ฯลฯ) ผ่านการวิเคราะห์ขั้นสูงและการเรียนรู้ของเครื่อง (คุกกี้ของผู้ใช้งานเฉพาะราย พฤติกรรมออนไลน์และการใช้คอมพิวเตอร์ ฯลฯ) ด้วยวิธีการเหล่านี้ ทีมป้องกันการทุจริตขององค์กรการเงินจะสามารถระบุได้อย่างถูกต้องว่าเป็นตัวเราจริงที่กำลังกรอกข้อมูลสำคัญของเรา หรือเป็นผู้ใช้บัตรปลอมที่กำลังพยายามซื้อสินค้าโดยใช้บัตรที่ขโมยมา เพื่อทำการอนุมัติหรือปฏิเสธธุรกรรมนั้น หรือส่งไปทำการวิเคราะห์เพิ่มเติม

อย่างไรก็ดี หน้ากากดิจิทัลสามารถถูกปลอมแปลงหรือสร้างขึ้นใหม่ทั้งหมดได้ และการสืบสวนของ แคสเปอร์สกี แล็บ พบว่าอาชญากรรมไซเบอร์กำลังพยายามใช้อัตลักษณ์ดิจิทัลปลอมนี้เพื่อหลบเลี่ยงมาตรการป้องกันการทุจริตขั้นสูง โดยในเดือนกุมภาพันธ์ 2019 งานวิจัยของแคสเปอร์สกี แล็บ เปิดเผยถึงตลาดเจเนซิส ดาร์กเน็ต (Genesis Darknet) ร้านค้าออนไลน์ที่จำหน่ายหน้ากากดิจิทัลและบัญชีผู้ใช้งานที่โจรกรรมมาในราคาตั้งแต่ 5-200 ดอลลาร์ต่อรายชื่อ ลูกค้าของร้านเพียงแค่ซื้อหน้ากากที่เพิ่งโจรกรรมมาพร้อมกับชื่อล็อกอินและรหัสผ่านที่ใช้กับร้านค้าและบริการชำระเงินออนไลน์ และเริ่มใช้งานผ่านการเชื่อมต่อเบราว์เซอร์และพร็อกซีเพื่อลอกเลียนกิจกรรมของผู้ใช้ตัวจริง หากพวกเขามีข้อมูลสำคัญของผู้ใช้ที่ถูกต้องตามกฎหมาย ผู้โจมตีก็สามารถเข้าถึงบัญชีออนไลน์หรือทำธุรกรรมรายการใหม่ที่เชื่อถือในนามของผู้ใช้รายนั้นได้ทันที

“เราเล็งเห็นถึงแนวโน้มที่ชัดเจนของการทุจริตผ่านบัตรเครดิตที่เพิ่มมากขึ้นทั่วโลก แม้อุตสาหกรรมบัตรเครดิตนี้ได้ทุ่มงบลงทุนอย่างมหาศาลเพื่อสร้างมาตรการป้องกันการทุจริต หากการปลอมแปลงอัตลักษณ์ดิจิทัลกลับเป็นเรื่องที่จับได้ยากมาก ทางเลือกหนึ่งในการป้องกันการแพร่ระบาดของการคุกคามนี้คือการปิดการทำงานโครงสร้างพื้นฐานระบบของผู้ปลอมแปลงเสีย เราจึงขอกระตุ้นหน่วยงานที่มีหน้าที่บังคับใช้กฎหมายทั่วโลก ให้ใส่ใจมากยิ่งขึ้นต่อปัญหาเรื่องนี้และร่วมมือกันต่อต้านอย่างจริงจัง” เซอร์จีย์ ลอซห์คิน นักวิจัยด้านความปลอดภัย แคสเปอร์สกี แล็บ กล่าว

นอกจากนี้ ยังมีเครื่องมืออื่น ๆ ที่ช่วยให้ผู้โจมตีสามารถสร้างหน้ากากดิจิทัลปลอมแบบพิเศษได้ใหม่ทั้งหมดซึ่งจะไม่กระตุ้นการทำงานของโซลูชั่นป้องกันการทุจริต ทีมนักวิจัยของแคสเปอร์สกี แล็บ ได้ตรวจสอบหนึ่งในเครื่องมือเหล่านั้น นั่นคือเบราว์เซอร์ Tenebris ชนิดพิเศษที่มีการฝังตัวสร้างองค์ประกอบสำเร็จรูปเพื่อการสร้างลายนิ้วมือแบบพิเศษ โดยเมื่อสร้างขึ้น ผู้ใช้บัตรก็เพียงเริ่มใช้งานหน้ากากนั้นได้อย่างง่าย ๆ ผ่านการเชื่อมต่อเบราว์เซอร์และพร็อกซี และใช้ดำเนินการธุรกรรมออนไลน์รูปแบบใด ๆ ก็ได้

แคสเปอร์สกี แล็บ จึงนำเสนอข้อปฏิบัติสำหรับธุรกิจต่าง ๆ เพื่อยกระดับความปลอดภัยด้วยมาตรการต่าง ๆ ดังต่อไปนี้

- เปิดการใช้งานการพิสูจน์อัตลักษณ์แบบหลายตัวแปรในการตรวจสอบความถูกต้องผู้ใช้งานในทุกขั้นตอน
- พิจารณาการใช้เครื่องมือรูปแบบใหม่สำหรับการยืนยันอัตลักษณ์เพิ่มเติม เช่น ข้อมูลชีวมิติ
- ใช้ระบบการวิเคราะห์พฤติกรรมผู้ใช้งานที่ทันสมัยที่สุด
- บูรณาการการแสดงฟีดข้อมูล Threat Intelligence เข้าสู่ระบบจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายองค์กร (SIEM) และการควบคุมด้านความปลอดภัยอื่น ๆ เพื่อให้ทราบถึงข้อมูลการคุกคามที่เกี่ยวข้องและทันสมัยที่สุด และเตรียมพร้อมสำหรับการโจมตีที่อาจเกิดขึ้นในอนาคต

บล็อกข่าวที่สรุปข้อมูลเรื่องการโจมตีด้วยอัตลักษณ์ดิจิทัลปลอม สามารถอ่านได้ ที่นี่ ในเรื่อง Securelist

เกี่ยวกับ แคสเปอร์สกี แล็บ
แคสเปอร์สกี้ แล็บ บริษัทระดับโลกผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ซึ่งก่อตั้งมานานกว่า 21 ปี มีความชำนาญพิเศษด้านภัยคุกคามที่ใช้เทคนิคเชิงลึก (Deep Threat Intelligence) และระบบการป้องกันรักษาความปลอดภัยของแคสเปอร์สกี้ แล็บ ได้ถ่ายทอดออกมาเป็นโซลูชั่นและบริการเพื่อการรักษาความปลอดภัยสำหรับปกป้องค์กรธุรกิจ โครงสร้างพื้นฐานที่สำคัญ องค์กรภาครัฐบาล และผู้บริโภคทั่วโลก ทั้งนี้กลุ่มผลิตภัณฑ์เพื่อรักษาความปลอดภัยที่ครอบคลุมของบริษัทประกอบด้วยโซลูชั่นและบริการเพื่อการป้องกันเอนด์พอยนท์ รวมทั้งโซลูชั่นเฉพาะทางมากมายเพื่อรับมือภัยคุกคามทางดิจิตอลที่วิวัฒนาการขยายขีดความซับซ้อนยิ่งขึ้นทุกวัน ปัจจุบันเทคโนโลยีของแคสเปอร์สกี้ แล็บ ทำหน้าที่ปกป้องผู้ใช้งานมากกว่า 400 ล้านคนทั่วโลก และเราได้ให้การช่วยเหลือลูกค้าองค์กรในการป้องกันสินทรัพย์ที่มีค่ายิ่งอีกมากกว่า 270,000 แห่งทั่วโลก ดูข้อมูลเพิ่มเติมได้ที่