กลุ่มจารกรรมข้อมูลแพลทินัมกลับมาอาละวาดอีกครั้ง โดยใช้วิทยาการอำพรางข้อมูลหลบหลีกการตรวจจับของระบบความปลอดภัย

นักวิจัยของแคสเปอร์สกี ได้เปิดเผยถึงปฏิบัติการจารกรรมทางไซเบอร์ที่มีความซับซ้อนสูงซึ่งมีเป้าหมายในการโจรกรรมข้อมูลของหน่วยงานทางการทูต รัฐบาล และการทหารในเอเชียตะวันออกเฉียงใต้ ปฏิบัติการนี้ดำเนินมาอย่างต่อเนื่องเกือบ 6 ปีและได้เชื่อมโยงเข้ากับการโจมตีซึ่งตรวจพบในภูมิภาคเมื่อเร็ว ๆ นี้ การตรวจสอบเพิ่มเติมกับเครื่องมือและขั้นตอนที่ใช้ในปฏิบัติการทำให้ทีมนักวิจัยพบข้อสรุปว่า ผู้โจมตีเบื้องหลังปฏิบัติการนี้คือกลุ่มแพลทินัม (PLATINUM) กลุ่มโจรกรรมทางไซเบอร์ที่นักวิจัยต่างคิดว่าสาบสูญไปนานแล้ว โดยในปฏิบัติการซึ่งไม่มีใครสังเกตเห็นมาเป็นเวลานานนี้ ทางกลุ่มได้ใช้วิธีการเข้ารหัสข้อมูลด้วยเทคนิคที่เรียกว่า วิทยาการอำพรางข้อมูล (Steganography) ซึ่งจะช่วยปกปิดการปรากฏของข้อมูลใด ๆ ในขั้นตอนการปฏิบัติการ

นักวิจัยด้านความปลอดภัยได้เคยให้คำเตือนถึงอันตรายของวิทยาการอำพรางข้อมูลไว้บ้างแล้ว โดยวิทยาการอำพรางข้อมูลคือการทำงานที่มีการถ่ายโอนข้อมูลด้วยการจัดรูปแบบข้อมูล (Format) ที่ถูกซ่อนไว้ ซึ่งจะช่วยปกปิดข้อเท็จจริงที่ว่ามีข้อมูลกำลังถูกส่งออกอยู่ในขณะนี้ ด้วยวิธีการทำงานเช่นนี้ วิทยาการอำพรางข้อมูลจึงแตกต่างจากการเข้ารหัสสัญญาณข้อมูล (Cryptography) ซึ่งเป็นเพียงการปกปิดข้อมูลเท่านั้น เมื่อใช้วิทยาการอำพรางข้อมูล ผู้จารกรรมข้อมูลจะสามารถแฝงตัวอยู่ในระบบที่ถูกเจาะได้เป็นเวลานานโดยไม่สร้างความน่าสงสัยใด ๆ ซึ่งวิธีนี้เป็นวิธีที่กลุ่มแพลทินัมใช้เพื่อคุกคามหน่วยงานรัฐบาลและองค์กรที่เกี่ยวข้องในเอเชียใต้และเอเชียตะวันออกเฉียงใต้ ซึ่งเป็นกลุ่มที่ถูกตรวจพบกิจกรรมคุกคามครั้งล่าสุดในปี ค.ศ. 2017

กรณีปฏิบัติการของกลุ่มแพลทินัมที่ได้รับการเปิดเผยเมื่อเร็ว ๆ นี้ก็คือ การตรวจพบคำสั่งของมัลแวร์ถูกฝังอยู่ในรหัส HTML ของเว็บไซต์ โดยปกติปุ่มแท็บ (Tab) และปุ่มเสปซบาร์ (Space bar) บนคีย์บอร์ดจะไม่เปลี่ยนแปลงเมื่อรหัส HTML ถูกใช้บนเว็บเพจ ดังนั้น ผู้คุกคามจึงเข้ารหัสคำสั่งด้วยลำดับการใช้งานของสองปุ่มนี้ ผลลัพธ์ก็คือการตรวจสอบชุดคำสั่งโจมตีในเครือข่ายแทบจะเป็นเรื่องที่เป็นไปไม่ได้เลย เนื่องจากมัลแวร์จะปรากฏเพียงในระดับการเข้าถึงเว็บไซต์ที่ต้องสงสัยเท่านั้น ซึ่งแทบจะไม่สามารถสังเกตเห็นได้เลยในเครือข่ายสัญญาณโดยรวม

โดยในการตรวจหามัลแวร์นี้ ทีมนักวิจัยต้องตรวจสอบโปรแกรมต่าง ๆ ที่มีความสามารถในการอัพโหลดไฟล์ข้อมูลเข้าสู่อุปกรณ์ได้ ซึ่งในจำนวนนั้น ผู้เชี่ยวชาญสังเกตพบว่ามีหนึ่งโปรแกรมที่ทำงานผิดปกติ ยกตัวอย่างเช่น

โปรแกรมนี้จะเข้าสู่ Dropbox ซึ่งเป็นบริการคลาวด์สาธารณะเพื่อทำการบริหารจัดการข้อมูลและถูกตั้งค่าให้ทำงานในบางช่วงเวลาเท่านั้น หลังจากนั้น ทีมนักวิจัยจึงตระหนักได้ว่า มันทำเช่นนี้เพื่อปกปิดกิจกรรมของมัลแวร์ท่ามกลางขั้นตอนการทำงานต่าง ๆ ในช่วงเวลาทำงานปกติ ซึ่งในช่วงเวลาทำงานปกตินั้น พฤติกรรมการทำงานของมันจะไม่ก่อให้เกิดความน่าสงสัยใดๆ เลย ซึ่งในความเป็นจริงนั้น ผู้ที่ใช้งานดาวน์โหลดกำลังทำให้ข้อมูลรั่วไหล ทั้งยังอัพโหลดข้อมูลและไฟล์ไปมากับอุปกรณ์ที่ติดมัลแวร์อยู่โดยไม่รู้ตัว

“นับตั้งแต่รับรู้ถึงการดำรงอยู่ของกลุ่มแพลทินัม ปฏิบัติการของกลุ่มล้วนมีความซับซ้อนและคิดค้นรูปแบบมาเป็นอย่างดี ซึ่งมัลแวร์ที่ใช้ในการโจมตีนี้ก็ไม่ใช่ข้อยกเว้น นอกเหนือจากวิทยาการอำพรางข้อมูล มันยังมีฟีเจอร์การทำงานอื่น ๆ ที่ช่วยให้มันสามารถโลดแล่นและทำงานรอดพ้นการตรวจจับได้เป็นเวลานาน ยกตัวอย่างเช่น มันสามารถถ่ายโอนคำสั่ง มิใช่เพียงจากศูนย์บัญชาการเท่านั้น แต่จากเครื่องที่ติดมัลแวร์เครื่องหนึ่งไปสู่อีกเครื่องหนึ่งได้ด้วยวิธีการนี้ มันจึงสามารถเข้าถึงอุปกรณ์ต่าง ๆ ที่เป็นส่วนหนึ่งในโครงสร้างพื้นฐานของอุปกรณ์ที่ติดมัลแวร์ซึ่งไม่ได้เชื่อมต่อกับอินเตอร์เน็ตได้ เมื่อพิจารณาทั้งหมดนี้แล้ว การค้นพบผู้คุกคามอย่างแพลทินัมที่ใช้วิทยาการอำพรางข้อมูล ถือเป็นสัญญาณเตือนว่า การคุกคามด้วยวิทยาการขั้นสูงที่แฝงตัวอยู่ได้นานกำลังเพิ่มระดับความซับซ้อนของกระบวนการทำงานเพื่อให้รอดพ้นการตรวจจับของเรดาร์ โดยผู้นำเสนอระบบความปลอดภัยต้องตระหนักสิ่งนี้ไว้เสมอในการพัฒนาโซลูชั่นด้านความปลอดภัย” อเล็กซีย์ ชูลมิน นักวิจัยด้านความปลอดภัยของแคสเปอร์สกี กล่าว

แคสเปอร์สกี นำเสนอมาตรการต่าง ๆ เพื่อช่วยลดความเสี่ยงของการตกเป็นเหยื่อปฏิบัติการอำพรางข้อมูล ดังนี้
• จัดการฝึกอบรมเพื่อสร้างความตระหนักรู้ด้านความปลอดภัยให้แก่พนักงาน โดยอธิบายถึงวิธีการตรวจสอบและหลีกเลี่ยงแอปพลิเคชั่นการทำงานหรือไฟล์ข้อมูลที่มีโอกาสติดมัลแวร์ ยกตัวอย่างเช่น พนักงานไม่ควรดาวน์โหลดหรือเปิดใช้งานแอปพลิเคชั่นหรือโปรแกรมใด ๆ จากแหล่งที่ไม่น่าเชื่อถือหรือไม่รู้จัก
• สำหรับการตรวจสอบการใช้งานระดับปลายสุด การตรวจสอบและการแก้ไขชุดเหตุการณ์ ให้ใช้โซลูชั่นอย่าง Kaspersky Endpoint Detection and Response
• นอกจากการปกป้องการใช้งานระดับปลายสุดที่สำคัญ ควรใช้โซลูชั่นด้านความปลอดภัยมาตรฐานระดับองค์กรเพื่อให้สามารถตรวจพบการคุกคามขั้นสูงในระดับเครือข่ายได้ตั้งแต่เนิ่นๆ อาทิ Kaspersky Anti Targeted Attack Platform

• มอบการเข้าถึงบริการข้อมูลข่าวกรองด้านการคุกคามใหม่ล่าสุด แก่ทีมงานศูนย์ปฏิบัติการเฝ้าระวังความปลอดภัยระบบเทคโนโลยีสารสนเทศ (Security Operation Center – SOC) ของคุณ เพื่อให้รับทราบถึงเครื่องมือ เทคนิค และกลวิธีใหม่ ๆ ของผู้คุกคามทางไซเบอร์ที่กำลังอุบัติขึ้น

ดูรายละเอียดทั้งหมดในรายงานได้ที่ Securelist.com

เกี่ยวกับ แคสเปอร์สกี แล็บ
แคสเปอร์สกี้ แล็บ บริษัทระดับโลกผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ซึ่งมีความชำนาญพิเศษด้านภัยคุกคามที่ใช้เทคนิคเชิงลึก (Deep Threat Intelligence) และระบบการป้องกันรักษาความปลอดภัยของแคสเปอร์สกี้ แล็บ

ได้ถ่ายทอดออกมาเป็นโซลูชั่นและบริการเพื่อการรักษาความปลอดภัยสำหรับปกป้ององค์กรธุรกิจ โครงสร้างพื้นฐานที่สำคัญ องค์กรภาครัฐบาล และผู้บริโภคทั่วโลก ทั้งนี้กลุ่มผลิตภัณฑ์เพื่อรักษาความปลอดภัยที่ครอบคลุมของบริษัทประกอบด้วยโซลูชั่นและบริการเพื่อการป้องกันเอนด์พอยนท์ รวมทั้งโซลูชั่นเฉพาะทางมากมายเพื่อรับมือภัยคุกคามทางดิจิตอลที่วิวัฒนาการขยายขีดความซับซ้อนยิ่งขึ้นทุกวัน ปัจจุบันเทคโนโลยีของแคสเปอร์สกี้ แล็บ ทำหน้าที่ปกป้องผู้ใช้งานมากกว่า 400 ล้านคนทั่วโลก และเราได้ให้การช่วยเหลือลูกค้าองค์กรในการป้องกันสินทรัพย์ที่มีค่ายิ่งอีกมากกว่า 270,000 แห่งทั่วโลก ดูข้อมูลเพิ่มเติมได้ที่ www.kaspersky.com